May 2020

13 email threat types to know about right now

How inbox defense protects against increasingly sophisticated attacks

Barracuda
Your journey, secured.

Table of Contents

Introduction: Radically reduce susceptibility to targeted email attacks

A cyberattack can affect your business in many ways, depending on its nature, scope, and severity. According to the FBI's Internet Crime Complaint Center (IC3), cybercrime cost $3.5 billion in losses in 2019 alone, with business email compromise (BEC) causing the most damages. That doesn't include unreported losses, which are significant. IC3 received 467,361 complaints last year—more than 1,300 per day—with phishing responsible for 93 percent of email breaches. There can be a variety of indirect and intangible costs from attacks, too, such as legal fees, regulatory fines, operational disruptions, a damaged brand reputation, and other severe consequences.

In today's rapidly evolving environment, traditional email security solutions aren't enough to protect businesses anymore. You must also effectively defend against sophisticated email threats that are often able to bypass defenses by using backdoor techniques, including spoofing, social engineering, and fraud, to penetrate networks and wreak havoc.

While comprehensive email gateway defenses provide a solid foundation, using a multilayered protection strategy radically reduces susceptibility to email attacks and helps better defend your business, data, and people.

This eBook takes an in-depth look at the top email threats, including their risks and impact on businesses, and how machine learning and API-based inbox defense can address the gaps in the email gateway and help provide total email protection against attacks.

"Through 2023, BEC attacks will continue to double each year to over $5 billion and lead to large financial losses for enterprises."

Source: Gartner, March 2020

Barracuda

Fighting increasingly complex email attacks

The email and phishing threats faced by organizations today vary greatly in complexity, volume, and the impact they have on businesses and their employees. There are a number of distinct categories of email threats:

- **Spam:** These are unsolicited, high-volume messages generally of a commercial nature, which are sent without regard to the recipient's identity.

- **Malware:** This is software specifically designed to cause damage to technical assets, disrupt operations, exfiltrate data, or otherwise gain access to a remote system. Malware is usually distributed through email attachments or URLs leading to malicious content.

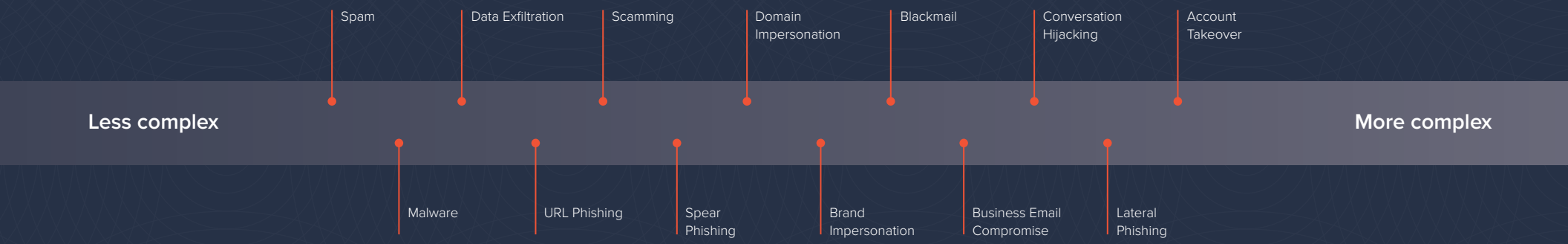
- **Data Exfiltration:** These types of attacks occur when data is copied or retrieved from a remote system without the owner's consent. It can occur maliciously or accidentally.

- **Phishing:** These emails attempt to trick an end user into believing the message is from a trusted person or organization to get them to take an action like disclosing credentials, wiring money, or logging into a legitimate account on an attacker's behalf.

- **Impersonation:** This category includes any attack where the malicious actor pretends to be a person, organization, or service. It's a broad superset of attacks that usually go hand in hand with phishing.

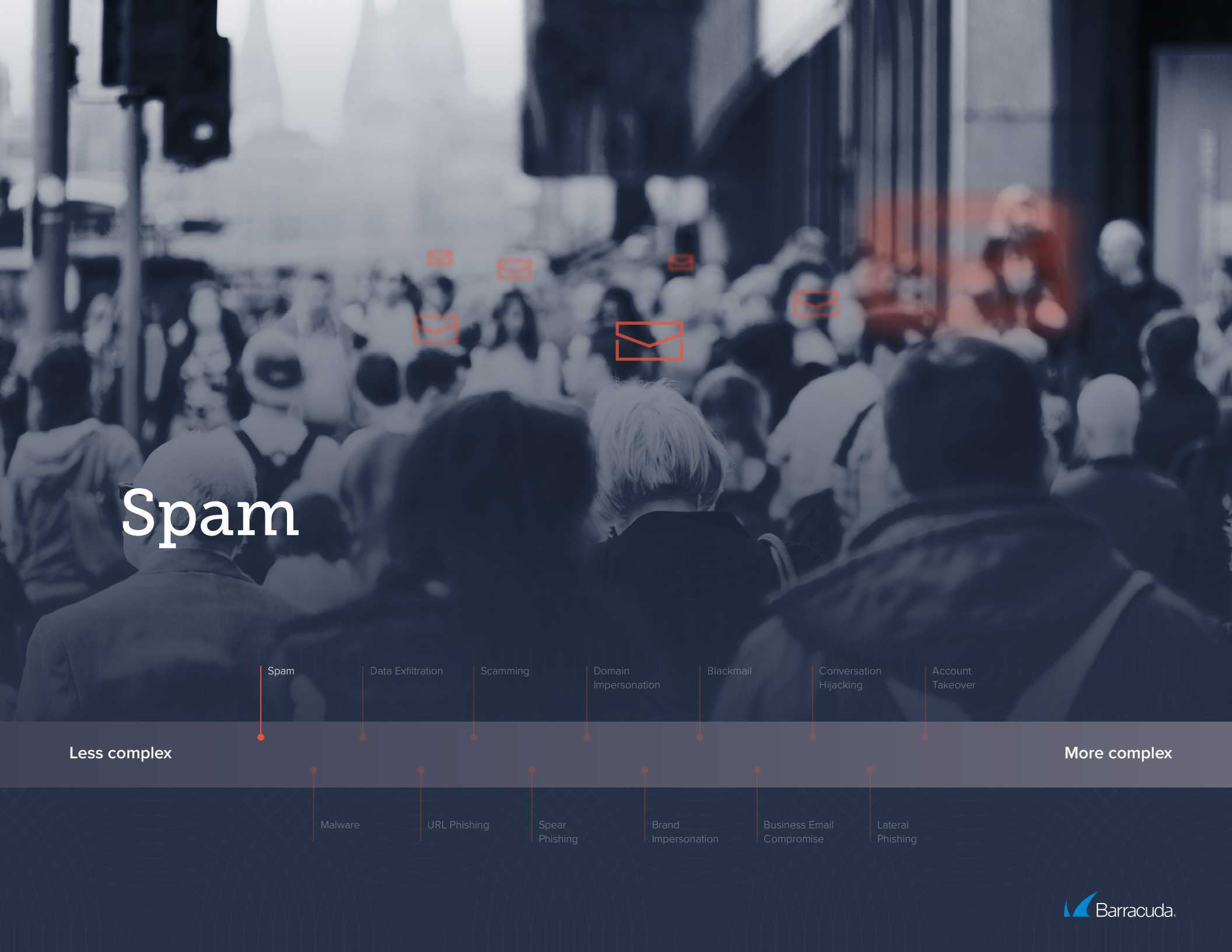
A total of 13 email threat types fall into these categories. Some of these attacks are used in conjunction with others; hackers often combine various techniques. For example, many spam messages include phishing URLs, and it's not uncommon to see a compromised account be used in internal or lateral wire fraud. Understanding the nature and characteristics of these attacks helps build the best protection for your business, data, and people.

Here's a look at the top 13 email threat types and how to strengthen your email security posture against them.



As email attacks get more complex, they become harder to defend against

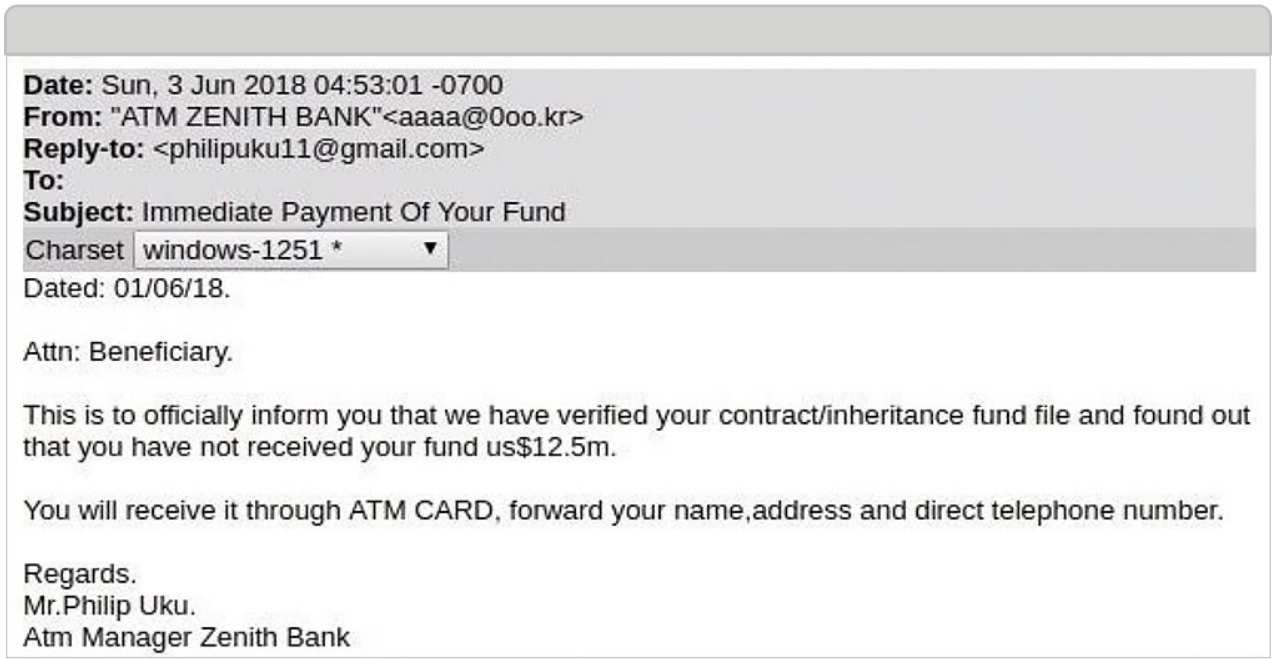
Barracuda


Spam
Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover
Less complex
More complex
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

Barracuda

Spam is unsolicited bulk email messages, also known as junk email. Spammers typically send an email to millions of addresses, with the expectation that only a small number will respond to the message. Spammers gather email addresses from a variety of sources, including using software to harvest them from address books. The collected email addresses are often also sold to other spammers.

Spam comes in various forms. Some spam emails push scams. Others are used to conduct email fraud. Spam also comes in the form of phishing emails that use brand impersonation to trick users into revealing personal information, such as login credentials and credit card details.



Date: Sun, 3 Jun 2018 04:53:01 -0700
From: "ATM ZENITH BANK"<aaaa@0oo.kr>
Reply-to: <philipuku11@gmail.com>
To:
Subject: Immediate Payment Of Your Fund
Charset windows-1251 *

Dated: 01/06/18.

Attn: Beneficiary.

This is to officially inform you that we have verified your contract/inheritance fund file and found out that you have not received your fund us$12.5m.

You will receive it through ATM CARD, forward your name,address and direct telephone number.

Regards.
Mr.Philip Uku.
Atm Manager Zenith Bank

Example of an attack

Barracuda

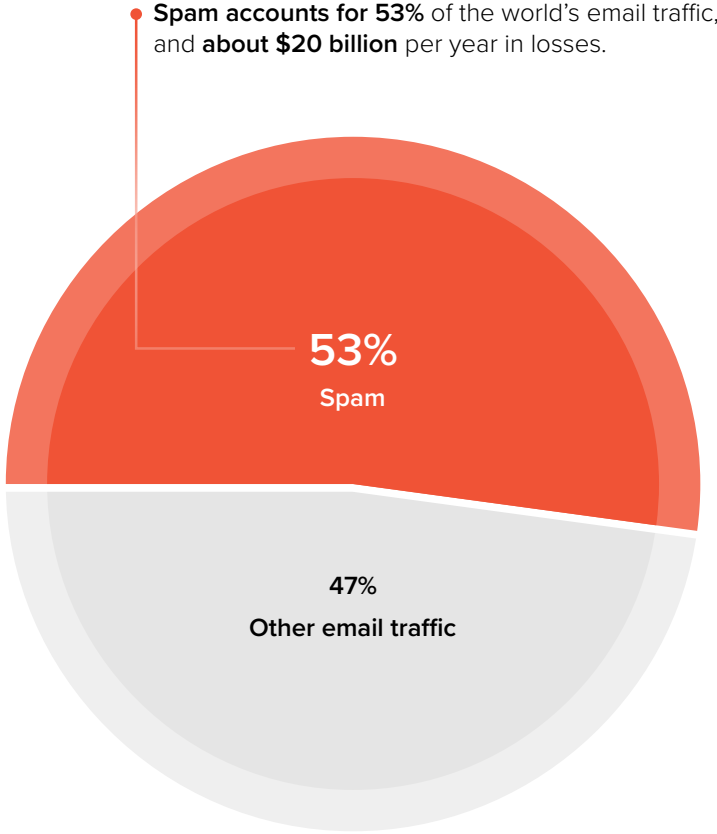
Impact of spam

Spam costs businesses about $20 billion per year in losses. It lowers productivity by flooding inboxes with junk mail and impacts server traffic to process messages. Spam can be used to distribute malware and in large-scale phishing attacks.

Strengthening email defense against spam

Modern gateways are very effective at blocking spam; inline deployment of spam filters helps stop spam before it hits the inbox.

API-based inbox defense isn't as effective against these large-scale attacks. Voluminous attacks, such as spam, can overwhelm email servers and have an adverse impact on inbox performance, creating a large inbox load before being clawed back by APIs.



Barracuda


Malware
Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover
Less complex
More complex
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing
Barracuda

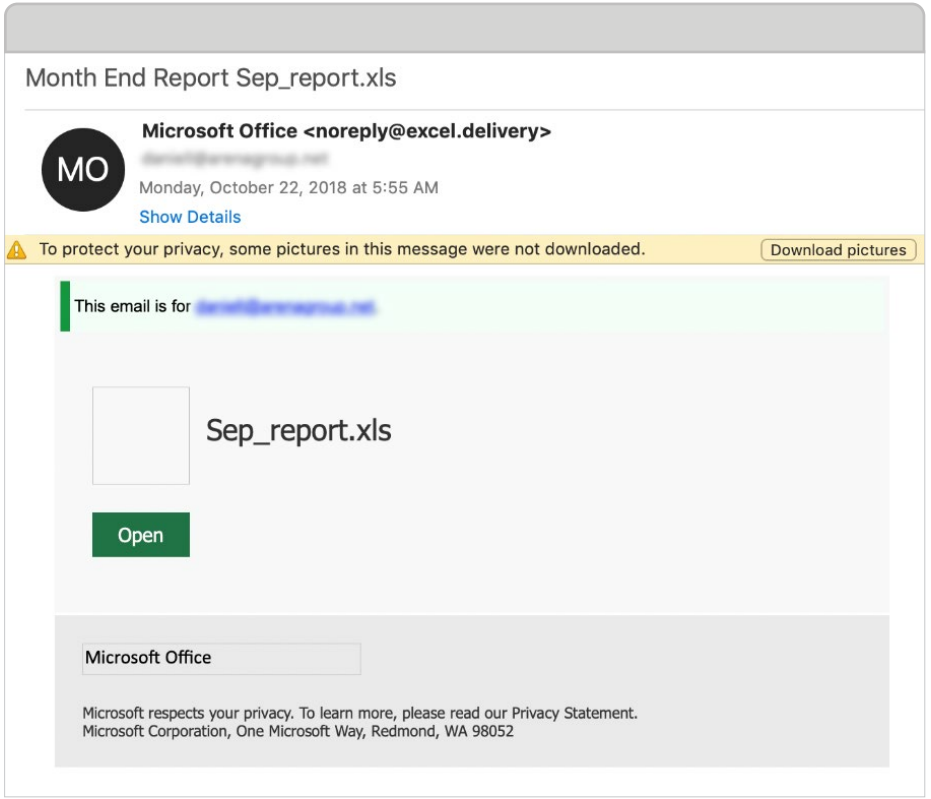
Cybercriminals use email to deliver documents containing malicious software, also known as malware. Typically, either the malware is hidden directly in the document itself, or an embedded script downloads it from an external website. Common types of malware include viruses, Trojans, spyware, worms, and ransomware.

Common types of malware attacks

Volumetric malware: This type of malware is designed to be spread en masse and take advantage of older, unpatched systems using common vulnerabilities. This type of malware exploits known vulnerabilities and can generally be caught by signatures and simple heuristics.

Zero-day malware: Advanced malware attacks use zero-day threats, which are ones that haven't been seen before and don't match any known malware signatures. They may exploit a previously unknown software vulnerability or use a new malware variant delivered by standard means. These zero-day attacks are impossible to detect with traditional signature-based solutions.

URL attacks: URLS that point to malicious websites or payloads are generally intended to trick users into clicking to download malware.



Example of an attack

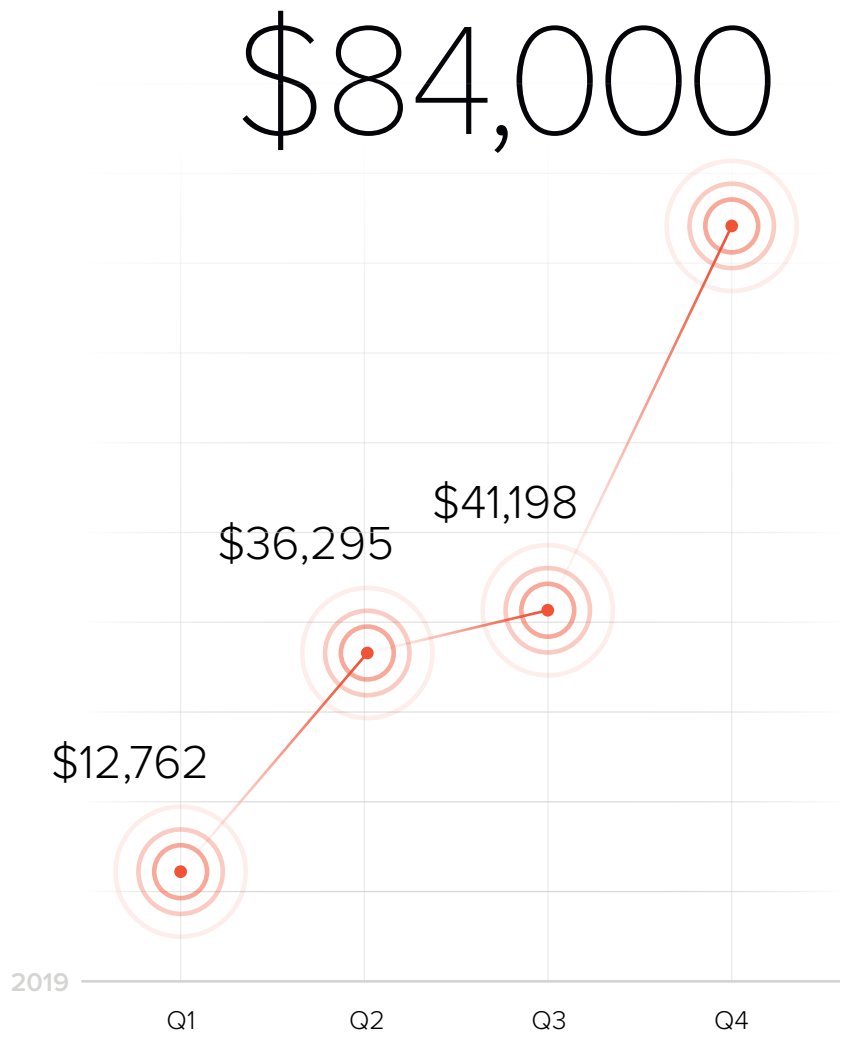
Barracuda

Impact of malware

94 percent of malware is delivered via email. With ransomware, one of the most popular forms of malware, cybercriminals infect the network and lock email, data, and other critical files until a ransom is paid. These evolving and sophisticated attacks are damaging and costly. They can cripple day-to-day operations, cause chaos, and result in financial losses from downtime, ransom payments, recovery costs, and other unbudgeted and unanticipated expenses.

In 2019, ransomware costs may have hit $170 billion, this number includes not only ransoms paid out but loss in productivity, data and other damages caused the attack. The average amount of ransom more than doubled from $41,198 in Q3 2019 to $84,000 in Q4 2019.

There were many well-publicized ransomware attacks in 2019 on businesses and government organizations. In government ransomware attacks, local, county, and state governments have all been targets, including schools, healthcare, libraries, courts, and other entities.

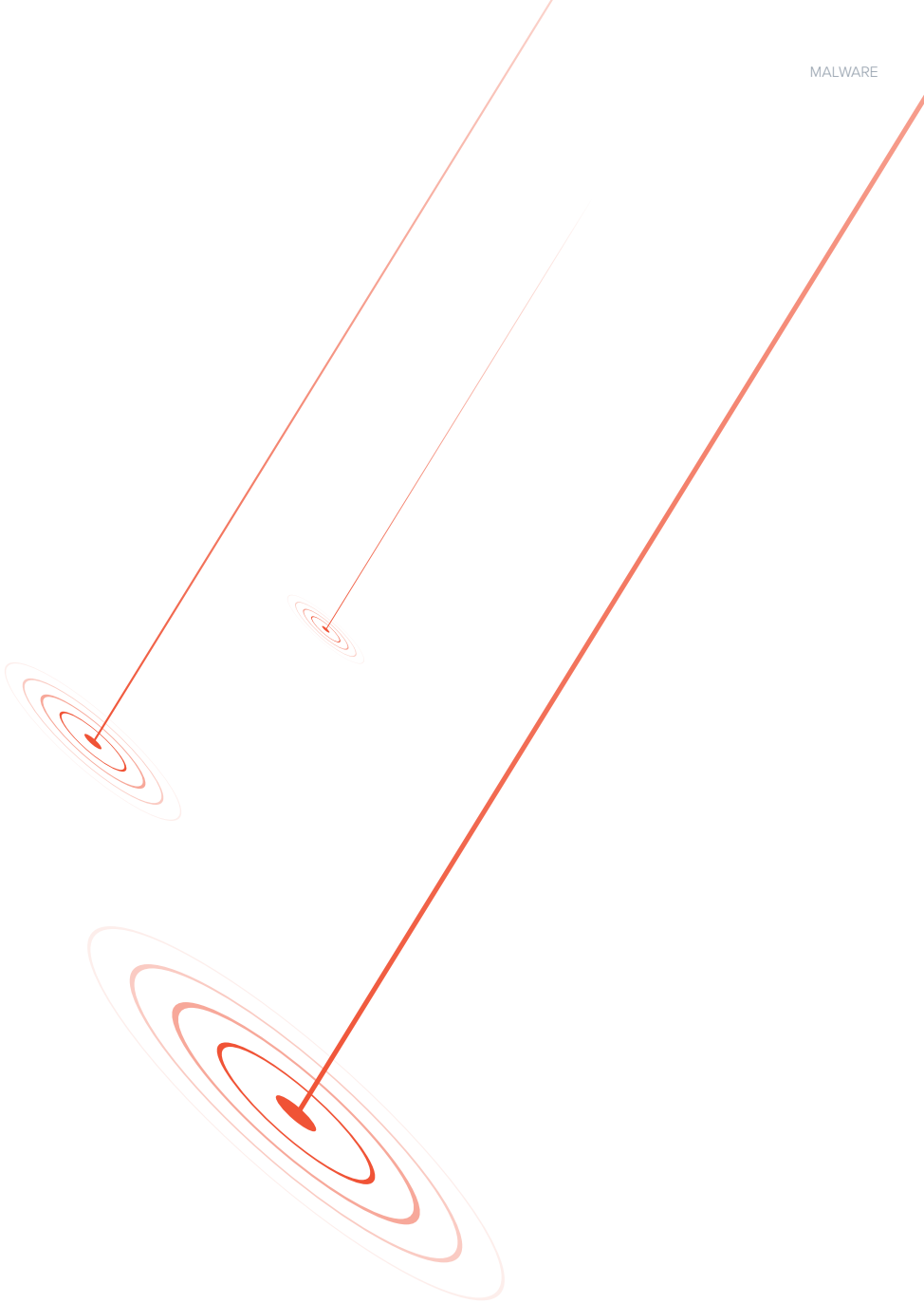


Average ransom amounts have exploded

Barracuda

Email defense against malware

Malware protection is best done at the gateway level, before emails hit inboxes. Signature matching remains an important tool to detect and block most malware variants. However, there are more advanced techniques available for detecting zero-day threats. Sandboxing is one such tool: Suspicious files and links are analyzed in an isolated test environment to make sure they are safe before being delivered to users' inboxes. New malware signatures can be created based on sandbox analysis, to help prevent future attacks.



Barracuda

Data Exfiltration

Spam | **Data Exfiltration** | Scamming | Domain Impersonation | Blackmail | Conversation Hijacking | Account Takeover

Less complex — **More complex**

Malware | URL Phishing | Spear Phishing | Brand Impersonation | Business Email Compromise | Lateral Phishing

Barracuda

Data exfiltration is the unauthorized transfer of data from a computer or other device. Also called data extrusion, data exportation, and data theft, data exfiltration can be conducted manually via physical access to a computer and as an automated process using malicious programming on the internet or a network. Attacks are typically targeted, with the objective of gaining access to a network or machine to locate and copy specific data. In addition to malicious attacks, data is frequently lost accidentally due to human error.

Impact of data exfiltration

According to an annual IBM report, the average total cost of a data breach was $3.92 million in 2019. For some industries, such as healthcare, this number can almost double. Data breaches in the United States were the most expensive, with an average cost of $8.19 million. The average size of a data breach was 25,575 records.

Data loss can lead to financial losses and have a long-lasting impact on an organization's reputation.

Average **cost** of a data breach in 2019

$3.92M

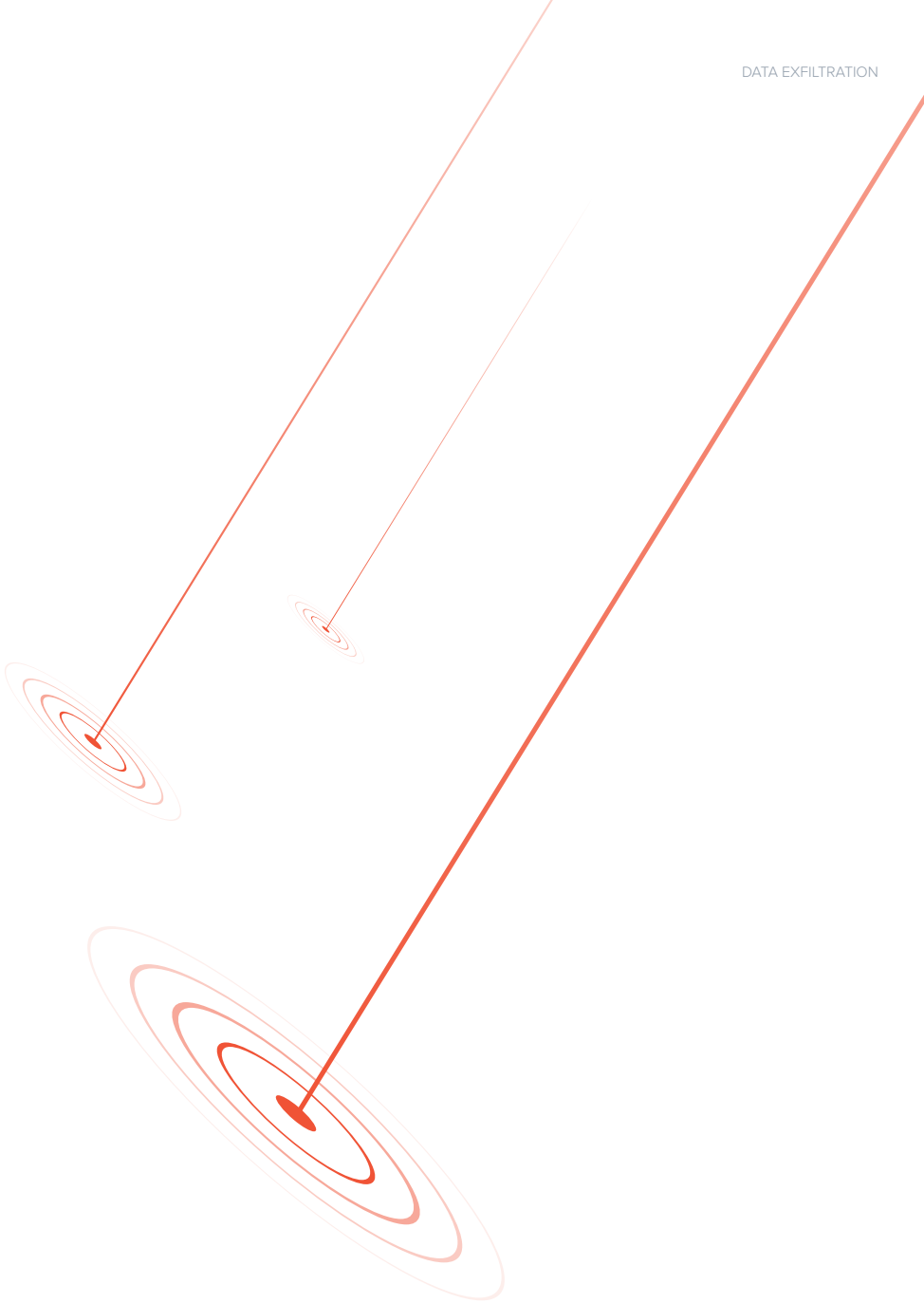
Average **size** of a data breach

25,575
records

Barracuda

Email defense against data exfiltration

Secure email gateways are deployed in-line with mail flow; they filter both inbound and outbound messages. Data loss prevention (DLP) is a set of technologies and business policies to make sure end users do not send sensitive or confidential data outside the organization. A DLP system scans all outbound email to look for pre-determined patterns that might indicate sensitive data, including credit card numbers, Social Security numbers, and HIPAA medical terms. Messages containing this type of sensitive data are automatically encrypted.



Barracuda

URL Phishing

Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover

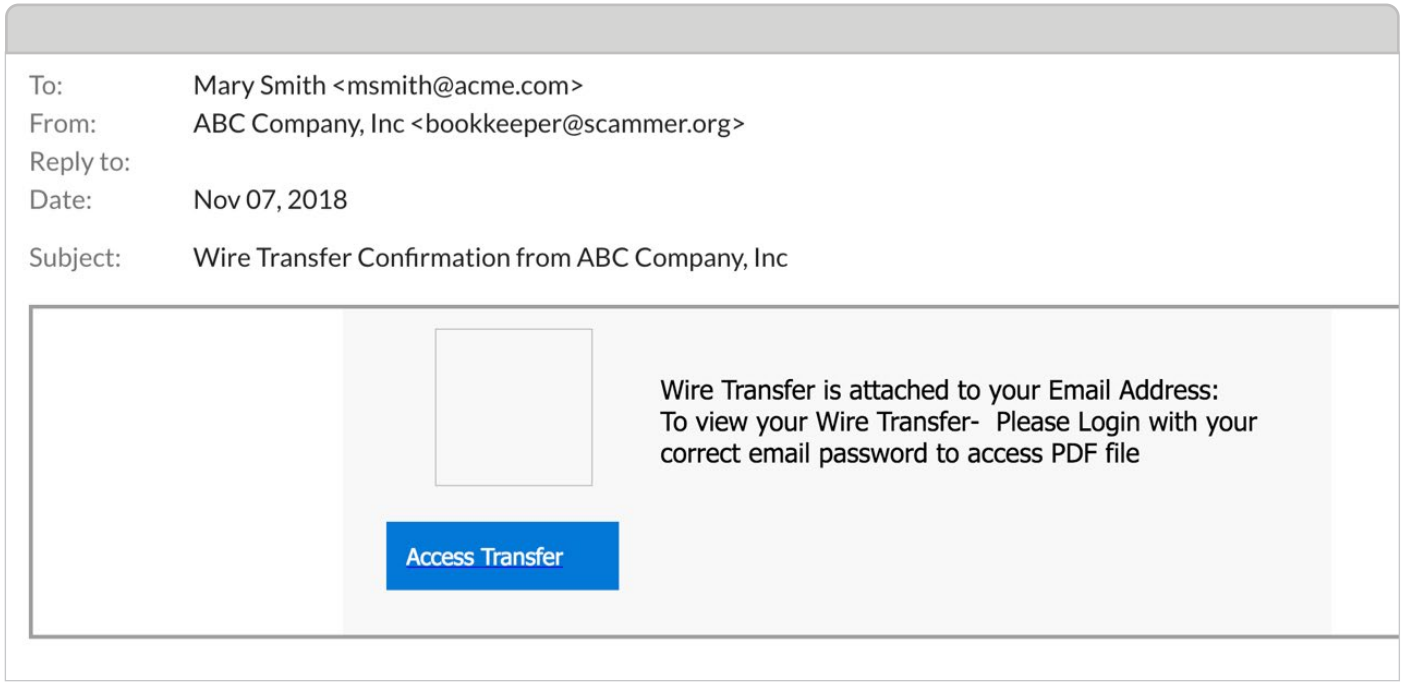
Less complex

More complex

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

Barracuda

In phishing attacks, cybercriminals try to obtain sensitive information for malicious use, such as usernames, passwords, or banking details. With URL phishing, cybercriminals use email to direct their victims to enter sensitive information on a fake website that looks like a legitimate website.



Example of an attack

Barracuda

Impact of URL phishing

About 32 percent of breaches involve phishing, and many phishing attacks include malicious links to fake websites. The use of URLs in phishing emails is popular and effective. Unfortunately, about 4 percent of recipients in any given phishing campaign click on the malicious link, and hackers only need one person to let them in.

Given the success rate, it's not surprising that reported losses in 2019 due to phishing reached almost $58 million. That's bad news, considering only 57 percent of organizations have URL protection in place, according to a recent survey.

Email defense against URL phishing

Gateways are very effective at protecting against mass URL phishing attacks. Gateways deploy URL filtering and URL re-write technologies to block access to malicious website links distributed via email, including all known malware and phishing sites. Sandboxing can also help block malicious links.

API-based inbox defense complements and completes the security a gateway provides. An API can enable a historical, internal view of actual URLs used by an organization. Abnormal or impersonating URLs, which signal phishing attacks, can be blocked. Even when a phishing website has never been used in previous campaigns or is hosted on a high-reputation domain, inbox defense can help protect against targeted spear-phishing attacks that use malicious URLs.

Scamming

Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover

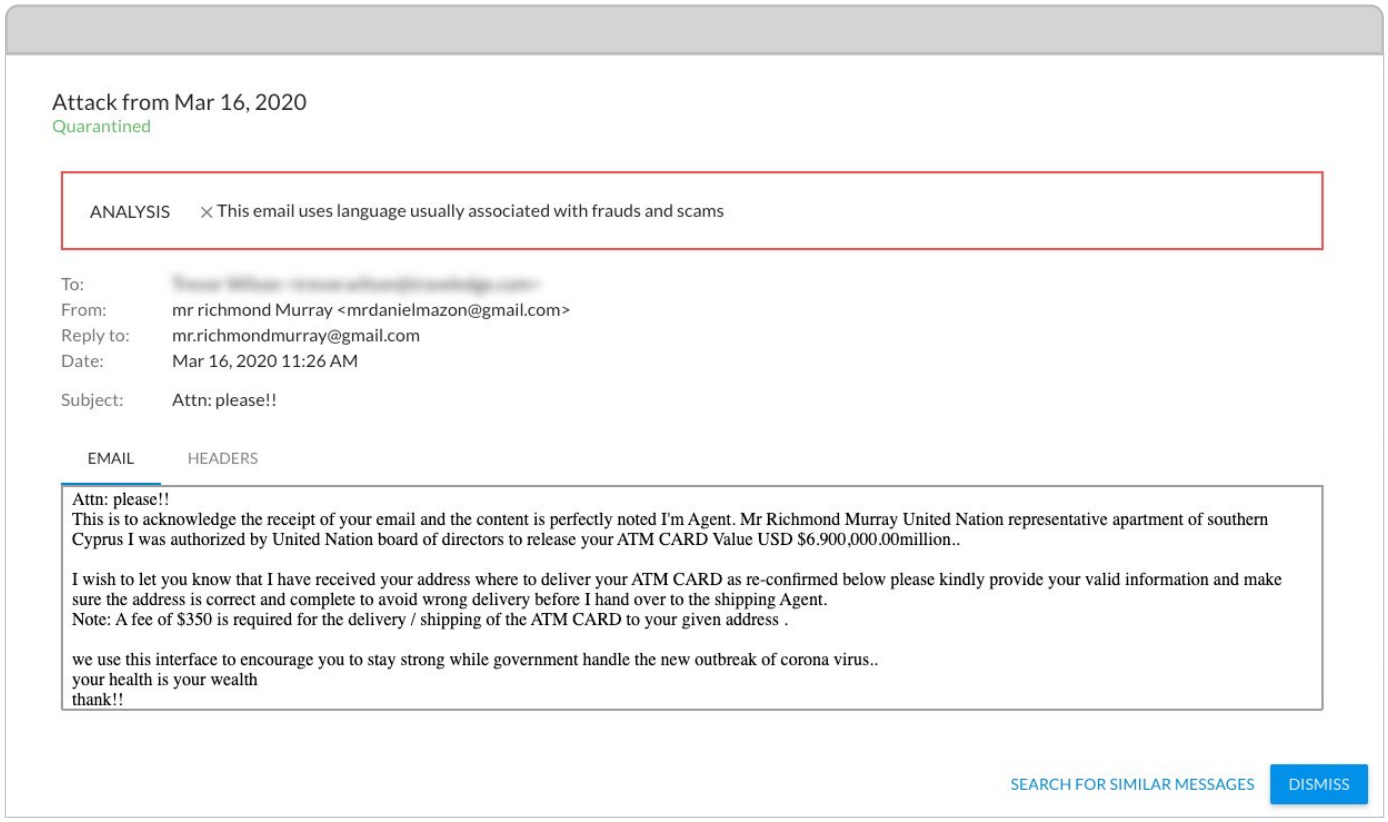
Less complex

More complex

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

Barracuda

With email scamming, cybercriminals use fraudulent schemes to defraud victims or steal their identity by tricking them into disclosing personal information. Examples of scamming include fake job postings, investment opportunities, inheritance notifications, lottery prizes, and fund transfers.

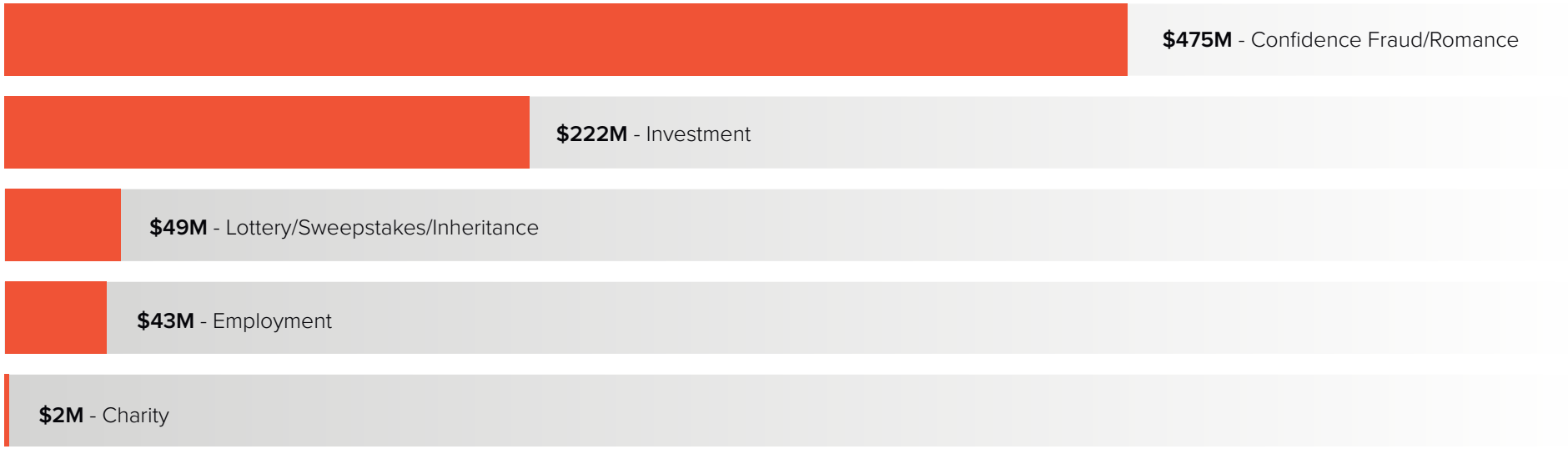


Example of an attack

Barracuda

Impact of scamming

Scamming accounts for 39 percent of all spear-phishing attacks. Scammers use a variety of different techniques, ranging from fake lottery wins to investment scams. It's not unusual for scammers to try to monetize tragedies, such as hurricanes, the COVID-19 crisis, and other disasters. Scammers prey on an individual's sympathy, charity, or fear. Unfortunately, many individuals fall for email scams, unwittingly sharing sensitive information or making payments to scammers. The FBI has recorded millions of dollars in reported losses as a result of these scams.



Scamming: Losses reported to the FBI in 2019

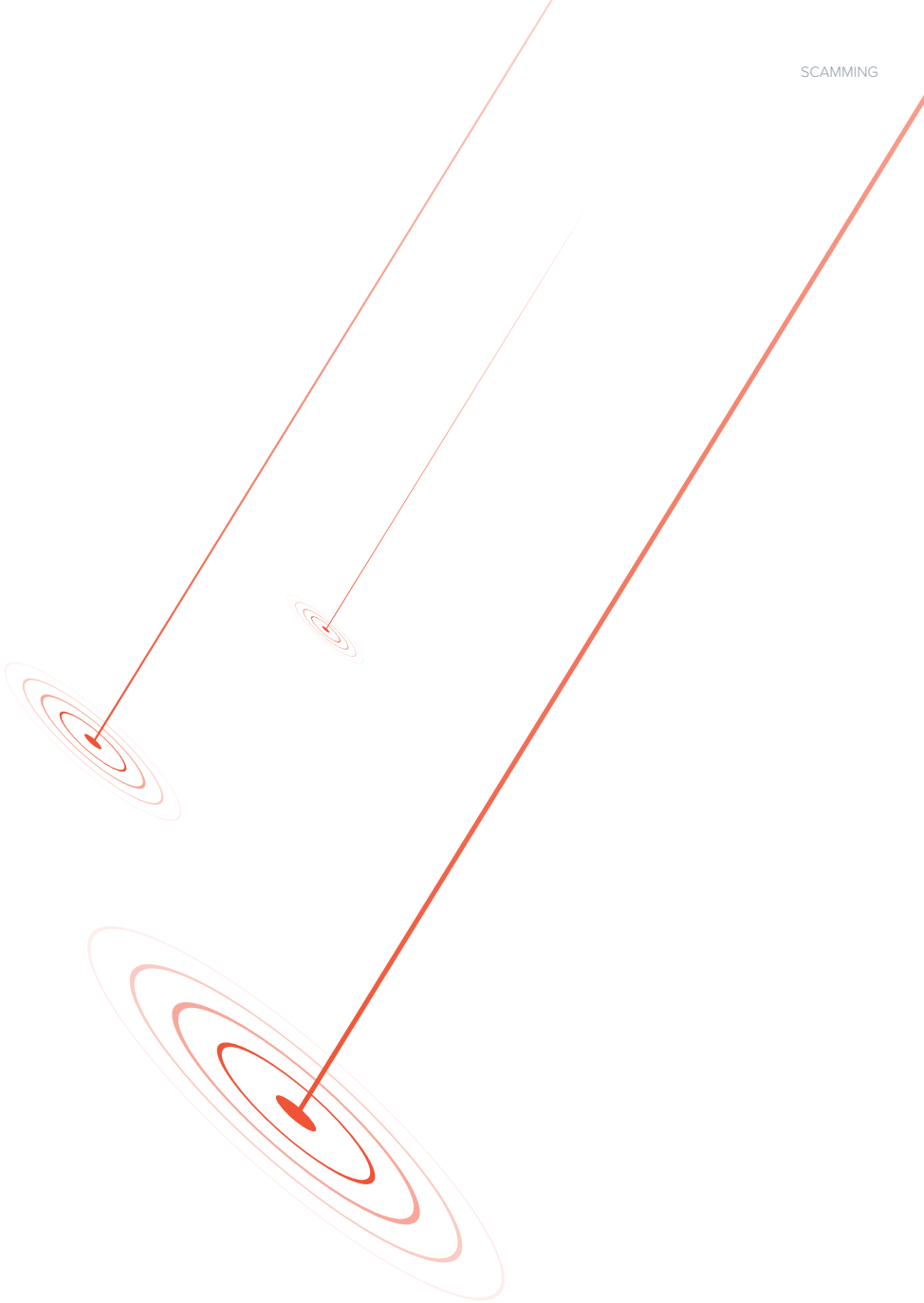
Barracuda

Email defense against scamming

API-based inbox defense against scamming uses historical email communications to determine what normal email communications look like for each employee. When criminals send scamming emails to their victims that fall outside of normal and expected communication, it's flagged and blocked by inbox defense.

Gateway solutions rely on granular policies, looking for specific keywords that indicate scams based on the content of the email. Combined with reputation filters and blacklists, this can be effective, but it often leads to false positives, preventing important messages from being delivered to users' inboxes.

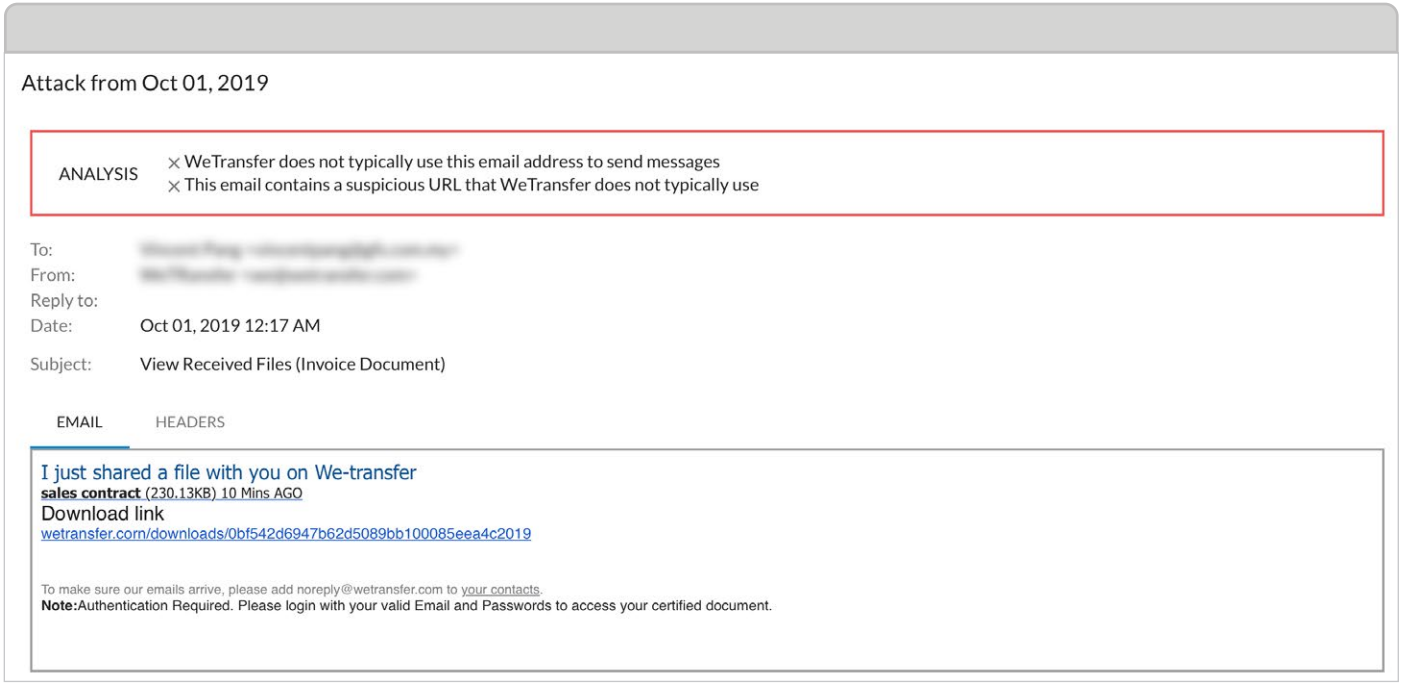
Many scamming emails can also be classified as spam. Organizations need to deploy both spam filters at email gateway and API-based inbox defense for effective protection against scamming.



Barracuda


Spear
Phishing
Spam
Data Exfiltration
Scamming
Domain
Impersonation
Blackmail
Conversation
Hijacking
Account
Takeover
Less complex
More complex
Malware
URL Phishing
Spear
Phishing
Brand
Impersonation
Business Email
Compromise
Lateral
Phishing
Barracuda

Spear-phishing is a highly personalized form of email phishing attack. Cybercriminals research their targets and craft carefully designed messages, often impersonating a trusted colleague, website, or business. Spear-phishing emails typically try to steal sensitive information, such as login credentials or financial details, which is then used to commit fraud, identity theft, and other crimes. Cybercriminals also take advantage of social-engineering tactics in their spear-phishing attacks, including urgency, brevity, and pressure, to increase the likelihood of success.



Example of an attack

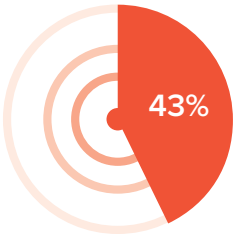
Barracuda

Impact of spear phishing

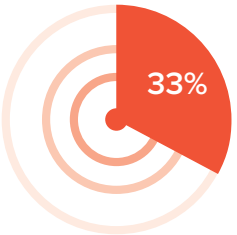
In Barracuda's recent Email Trends survey, 43 percent of organizations said they had been victims of a spear-phishing attack in the past 12 months. However, only 23 percent of organizations said they have dedicated spear-phishing protection in place.

When organizations fall victim to spear-phishing attacks, the impacts include malware infection of their machines and the network, direct monetary losses through wire transfers, and reputational damage. In many cases, spear-phishing attacks lead to the theft of credentials and email account takeover. Compromised accounts are often used to launch subsequent spear-phishing attacks. Organizations need dedicated spear-phishing protection to stop this vicious cycle.

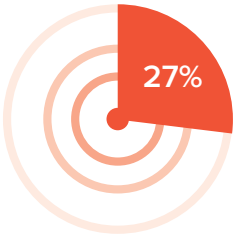
How businesses were affected by spear-phishing attacks in 2019[1]



Machines infected with malware or viruses

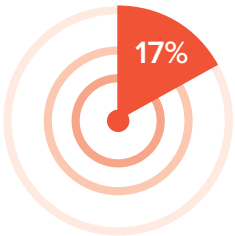


Stolen login credentials and/or account takeover



Reputational Damage

Direct monetary loss (e.g. money transferred)



Sensitive or confidential data stolen

There was no impact

Other **(3%)**

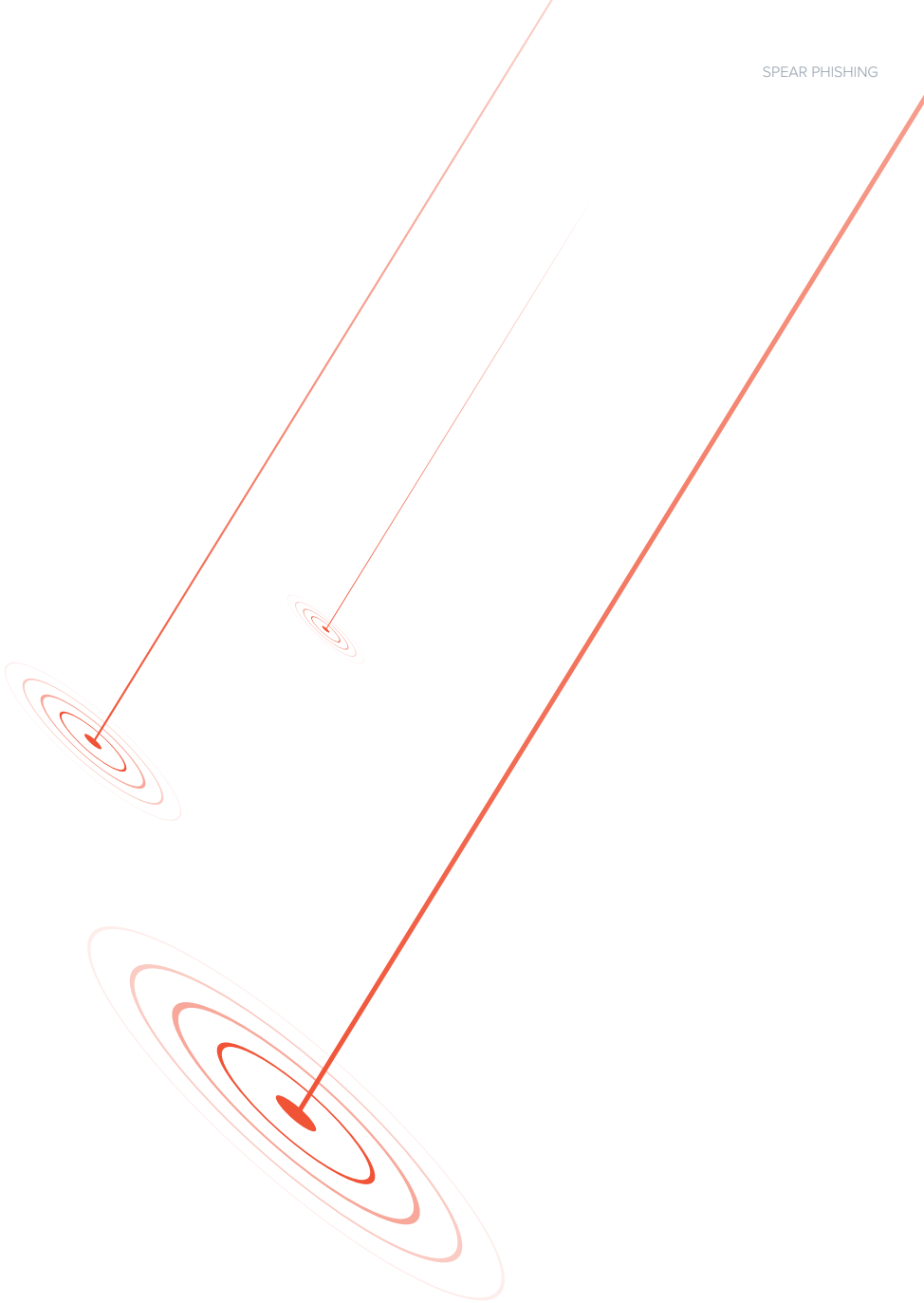
1 2019 Email Security Trends

Barracuda

Email defense against spear phishing

API-based inbox defense uses access to historical email communication data to build a communication identity graph, a statistical model that is specific to each user in the organization. This identity graph is then used to detect unusual communication patterns that fall outside of its statistical model, which in turn predicts and blocks spear-phishing attacks that make it past the gateway.

Traditional email security gateways have no visibility into historical data. Therefore, they evaluate each email based on a set of predetermined policies, filters, and signatures, rather than on historical communication and context. Spear-phishing attacks are designed to bypass these filters and policies and therefore often delivered to users inboxes.



Barracuda

Domain Impersonation

Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover

Less complex

More complex

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

Barracuda

Domain impersonation is often used by hackers as part of a conversation-hijacking attack. Attackers attempt to impersonate a domain by using techniques such as typosquatting, replacing one or more letters in a legitimate email domain with a similar letter or adding a hard-to-notice letter to the legitimate email domain. In preparation for the attack, cybercriminals register or buy the impersonating domain.

Domain impersonation is a very high-impact attack. It can be easy to miss the subtle differences between the legitimate email domain and the impersonated email domain. For example, an attacker trying to impersonate barracudanetworks.com would use a very similar URL:

barraeuda.com

barracada.com

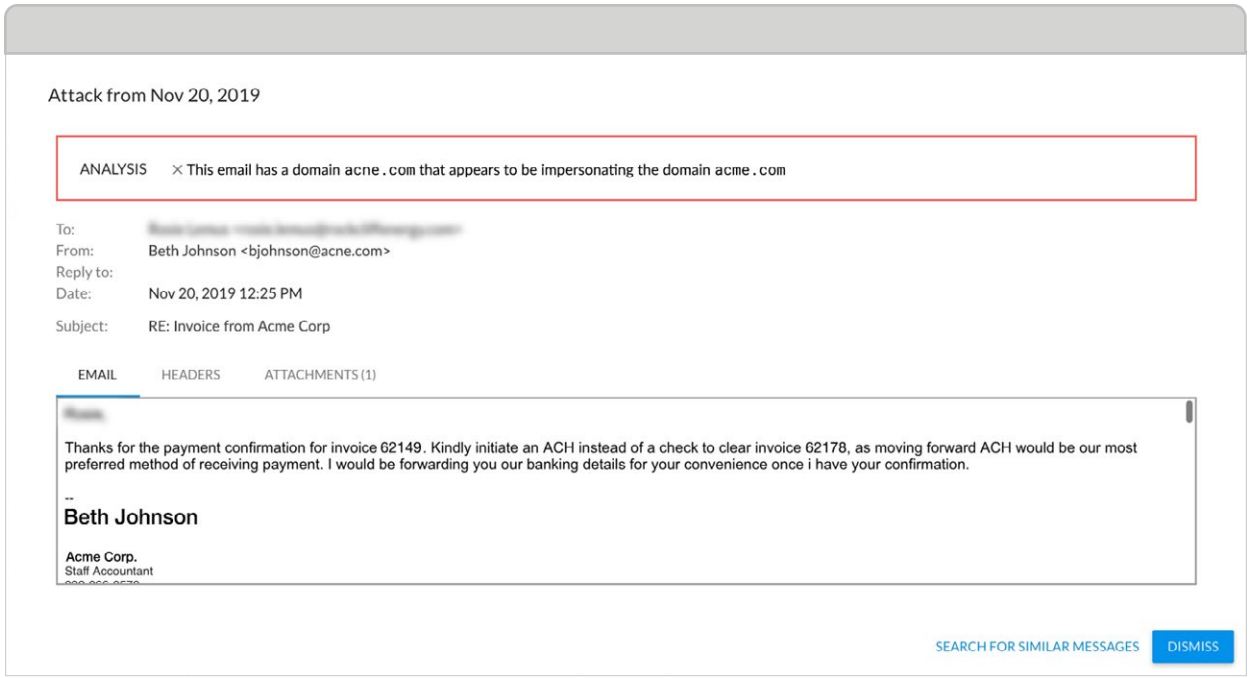
barracúda.com

barrracud.com

Sometimes, an attacker changes the top-level domain (TLD), using .net or .co instead of .com, to fool victims:

barracuda.net

barracuda.co



Example of an attack

Impact of domain impersonation

In recent months, Barracuda researchers have seen a sharp rise in domain-impersonation attacks used to facilitate conversation hijacking. An analysis of about 500,000 monthly email attacks shows a 400-percent increase in domain-impersonation attacks used for conversation hijacking.

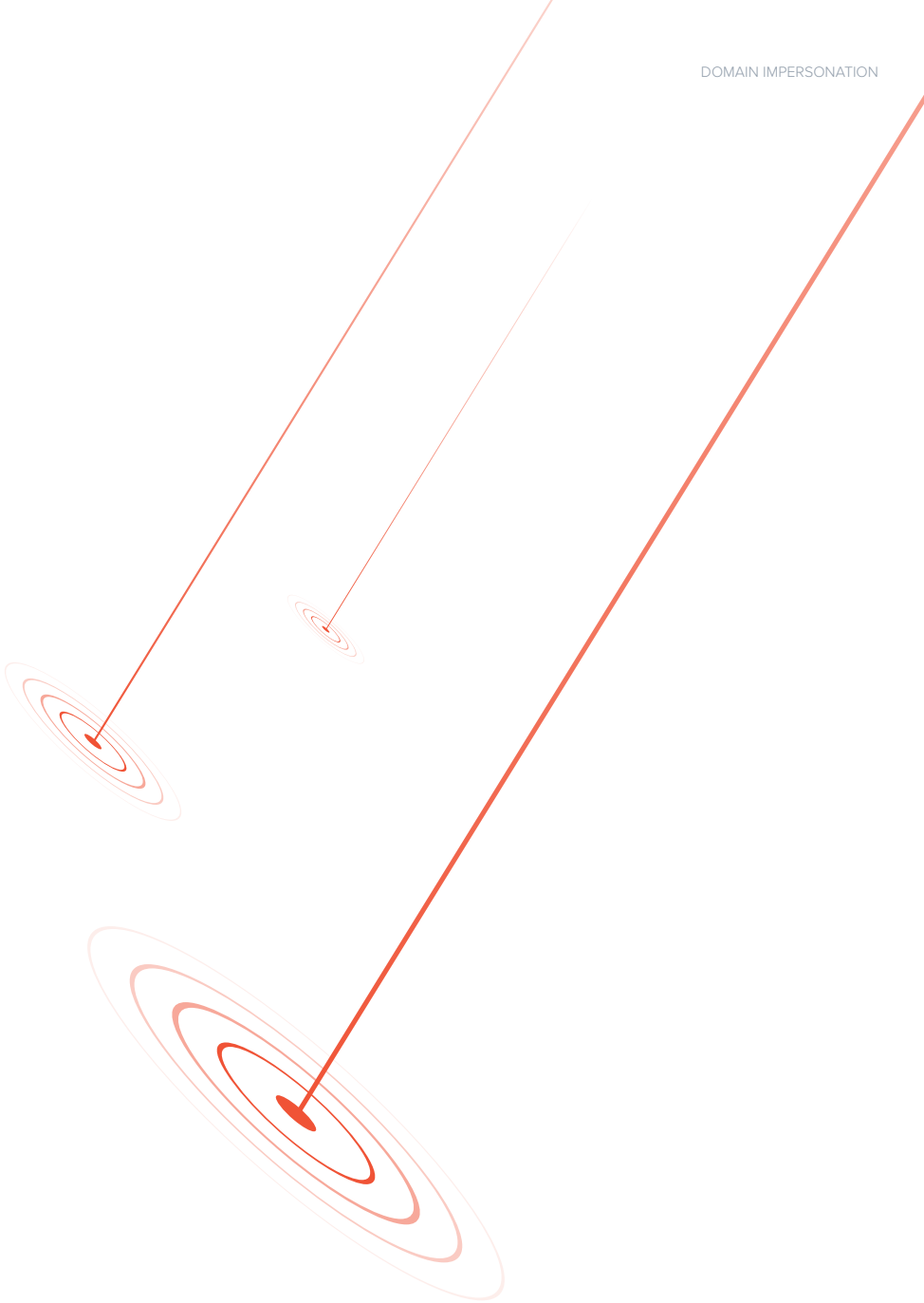
+400%

Barracuda

Email defense against domain impersonation

The biggest challenge with domain impersonation is accurately detecting typosquatted domains and differentiating an impersonation attempt from a real website. Email gateways must build lists of domains used by organizations and their partners over time, a long process that is prone to error and needs continuous management and updates. With so many email domains and variations, using gateways to detect domain impersonation leads to large numbers of false positives while also letting attacks through.

An API-based inbox defense uses past email communications to get data on domains used by the organization, their partners, and customers. Inbox defense associates specific conversations, requests, and individuals with specific email domains. So, when a vendor sends an unusual request from the wrong domain, inbox defense detects and blocks it.



Barracuda

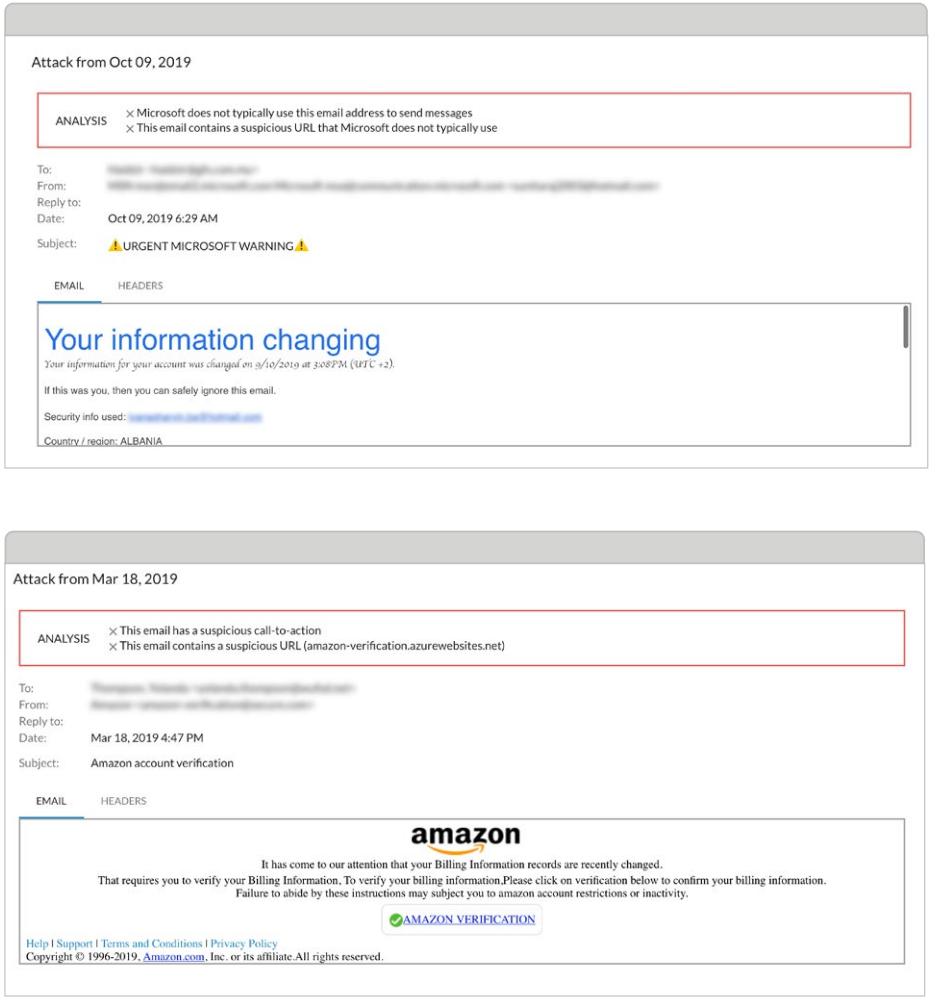

Brand
Impersonation
Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover
Less complex
More complex
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing
Barracuda

Brand impersonation is designed to impersonate a company or a brand to trick their victims into responding and disclosing personal or otherwise sensitive information.

Common types of brand impersonation include:

Service impersonation is a type of spear-phishing attack designed to impersonate a well-known company or commonly used business application. It is a popular type of spear-phishing attack because the emails are well designed as an entry point to harvest credentials and carry out account takeover. Brand impersonation attacks are also used to steal personally identifiable information, such as credit card and Social Security numbers.

Brand hijacking, also known as domain spoofing, is a common form of phishing. It occurs when an attacker appears to use a company's domain to impersonate a company or one of its employees. This is usually done by sending emails with false, or spoofed, domain names that appear to be legitimate.



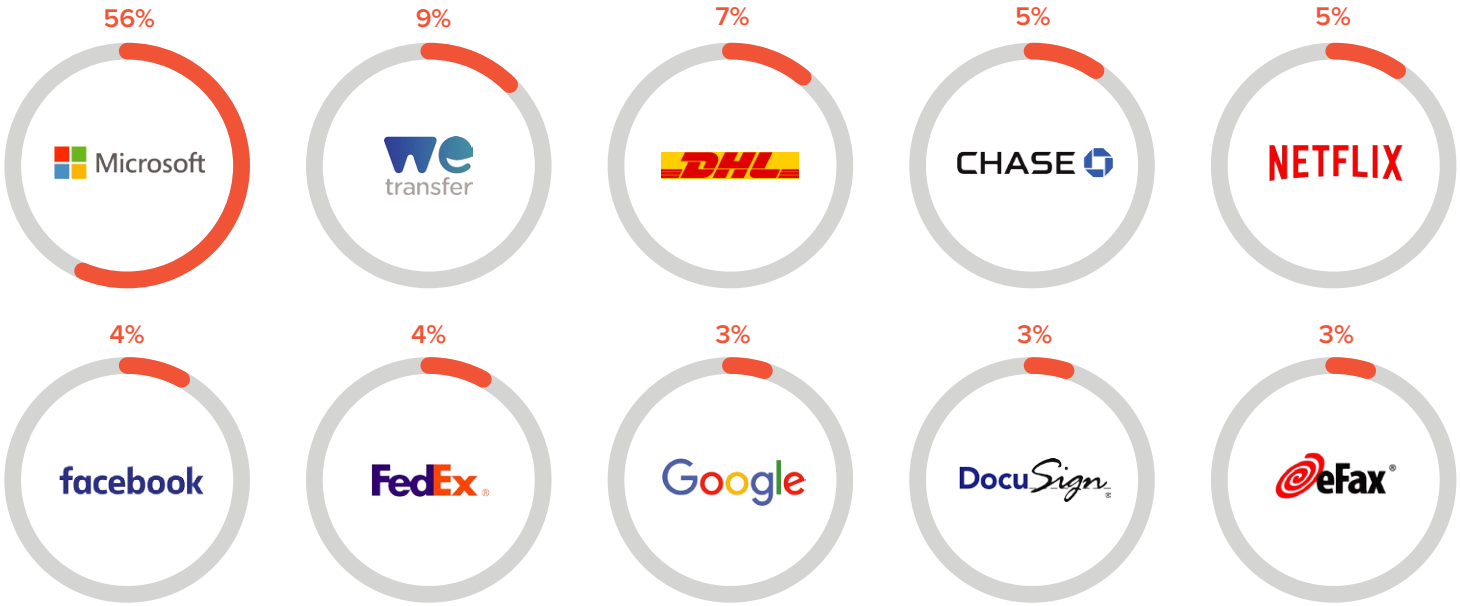
Examples of an attack

Barracuda

Impact of brand impersonation

Service impersonation is used in 47 percent of all spear-phishing attacks. Microsoft is the most impersonated brand in spear-phishing attacks. Impersonating Microsoft is one of the most common techniques used by cybercriminals to take over an account. Microsoft and Office 365 credentials are high value because they allow hackers to penetrate organizations and launch additional attacks.

Brand hijacking or spoofing attacks are made possible by a weakness in the email RFC standard that doesn't require full authentication of sending domains. Standards like DKIM, SPF, and DMARC make it much more difficult to launch these attacks. However, domain spoofing is widely used by hackers in impersonation attacks. A recent study showed that there are almost 30,000 spoofing attacks each day. Plus, 77 percent of Fortune 500 companies do not have DMARC policies set up, making it easy for scammers to spoof their brands in phishing attacks.



Most frequently impersonated brands

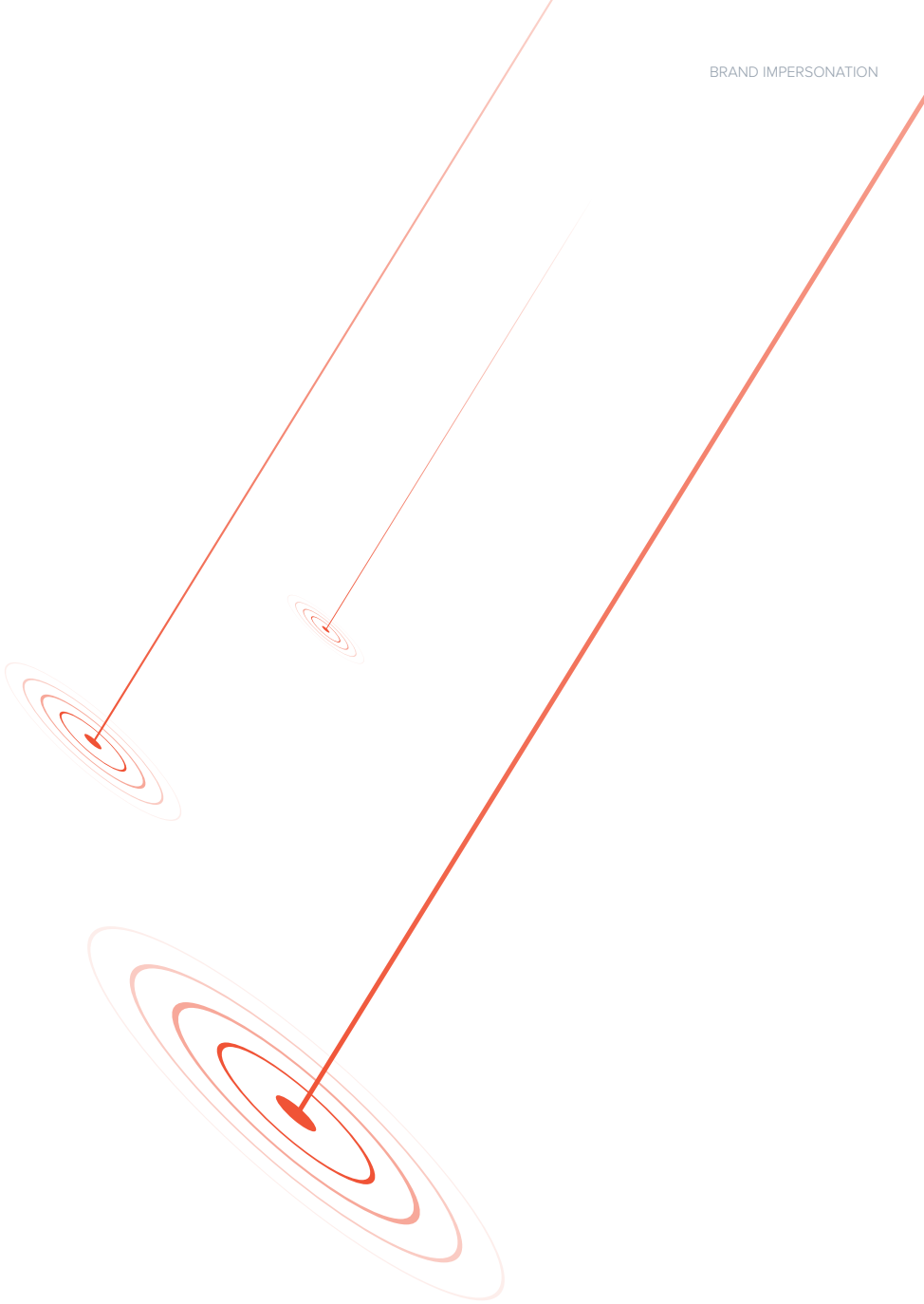
Barracuda

Email defense against brand impersonation

An API-based inbox defense against service impersonation uses past and internal email messages to get visibility into the services used by an organization. The data is used in a statistical detection model to understand the difference between fake and legitimate emails, including the branding and images of the legitimate services used by an organization.

Gateways have no such visibility into the services used by an organization and can't recognize the specific branding and images used by legitimate brands. They rely on predetermined policies, an approach that doesn't scale given the variety of service-impersonation attacks. API-based inbox defense is more effective at blocking service impersonation attacks.

Organizations can get visibility into domain fraud using DMARC authentication to protect against domain spoofing and brand hijacking. DMARC reporting provides visibility into how an email domain is used, which in turn allows an organization to set up DMARC enforcement policies that will prevent spoofing of the domain.

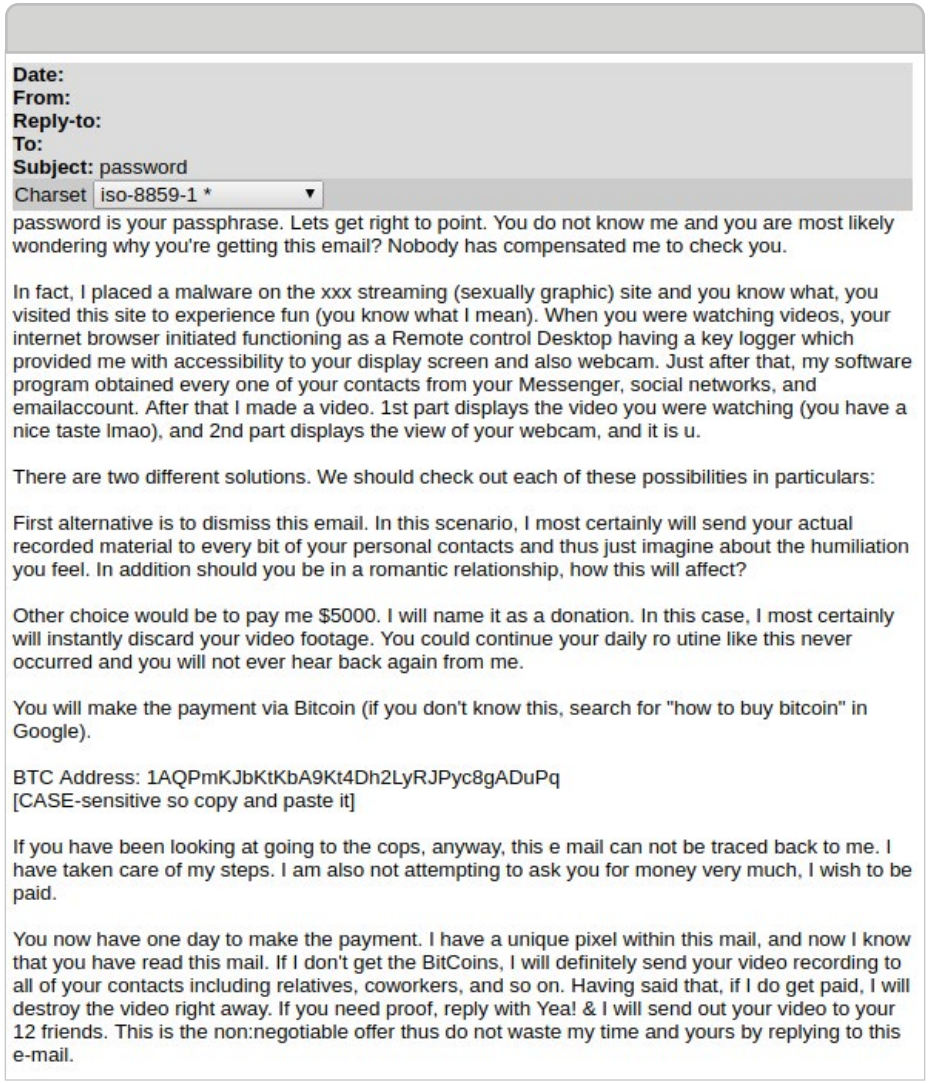


Barracuda


Blackmail
Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover
Less complex
More complex
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

Blackmail scams, including sextortion, are increasing in frequency, becoming more sophisticated, and bypassing email gateways.

In sextortion attacks, cybercriminals leverage usernames and passwords stolen in data breaches, using the information to contact and try to trick victims into giving them money. The scammers claim to have a compromising video, allegedly recorded on the victim's computer, and threaten to share it with all their contacts unless they pay up.



Date:
From:
Reply-to:
To:
Subject: password
Charset iso-8859-1 *

password is your passphrase. Lets get right to point. You do not know me and you are most likely wondering why you're getting this email? Nobody has compensated me to check you.

In fact, I placed a malware on the xxx streaming (sexually graphic) site and you know what, you visited this site to experience fun (you know what I mean). When you were watching videos, your internet browser initiated functioning as a Remote control Desktop having a key logger which provided me with accessibility to your display screen and also webcam. Just after that, my software program obtained every one of your contacts from your Messenger, social networks, and emailaccount. After that I made a video. 1st part displays the video you were watching (you have a nice taste lmao), and 2nd part displays the view of your webcam, and it is u.

There are two different solutions. We should check out each of these possibilities in particulars:

First alternative is to dismiss this email. In this scenario, I most certainly will send your actual recorded material to every bit of your personal contacts and thus just imagine about the humiliation you feel. In addition should you be in a romantic relationship, how this will affect?

Other choice would be to pay me $5000. I will name it as a donation. In this case, I most certainly will instantly discard your video footage. You could continue your daily ro utine like this never occurred and you will not ever hear back again from me.

You will make the payment via Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address: 1AQPmKJbKtKbA9Kt4Dh2LyRJPyc8gADuPq
[CASE-sensitive so copy and paste it]

If you have been looking at going to the cops, anyway, this e mail can not be traced back to me. I have taken care of my steps. I am also not attempting to ask you for money very much, I wish to be paid.

You now have one day to make the payment. I have a unique pixel within this mail, and now I know that you have read this mail. If I don't get the BitCoins, I will definitely send your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I do get paid, I will destroy the video right away. If you need proof, reply with Yea! & I will send out your video to your 12 friends. This is the non:negotiable offer thus do not waste my time and yours by replying to this e-mail.

Example of an attack

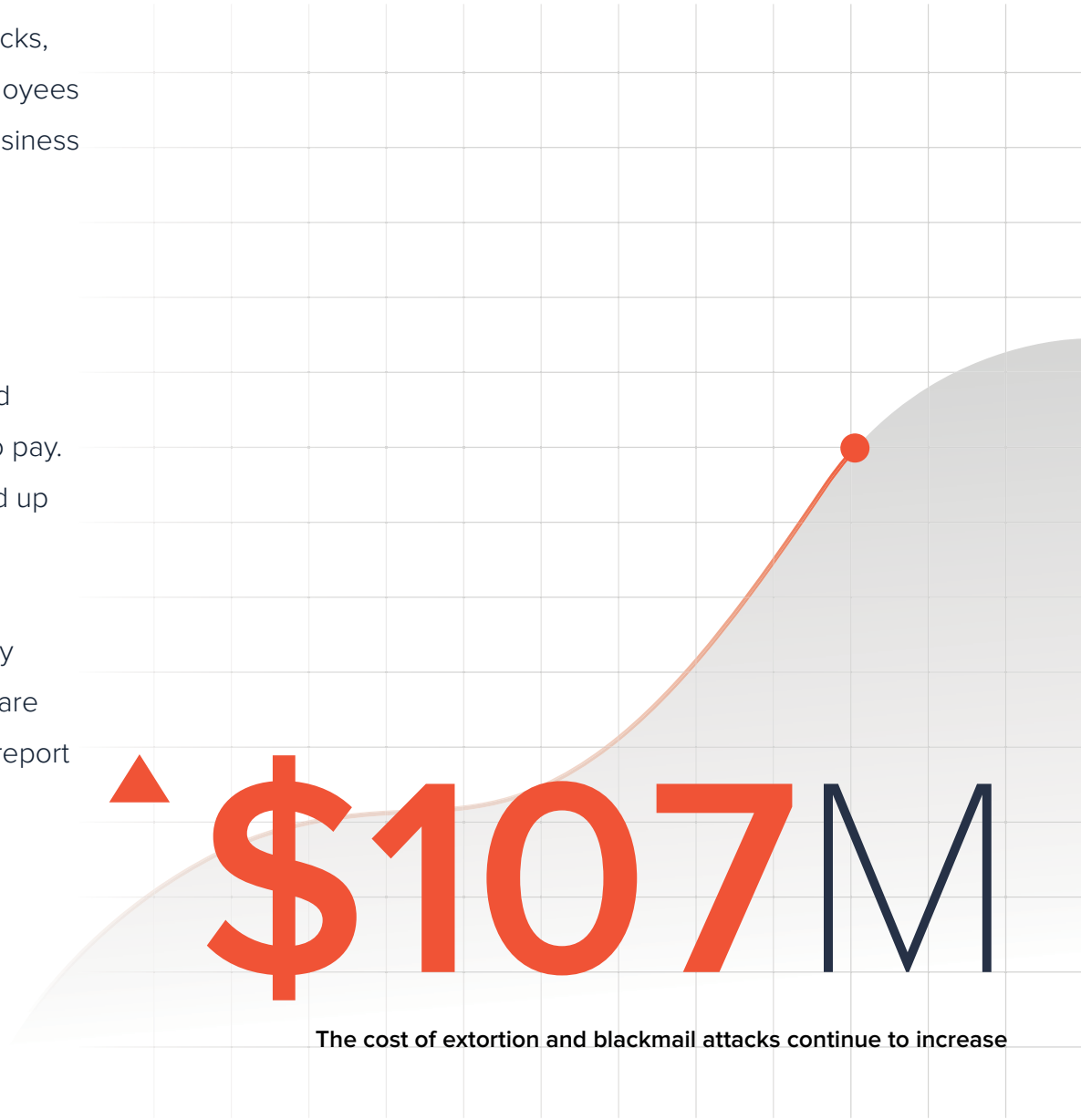
Barracuda

Impact of blackmail

Blackmail makes up about 7 percent of spear-phishing attacks, the same percentage as business email compromise. Employees are just as likely to be targeted in a blackmail scam as a business email compromise attack.

According to the FBI, the cost of extortion attacks, which includes blackmail, was more than $107 million in 2019. On average, attackers ask for a few hundred or a few thousand dollars, an amount that an individual would likely be able to pay. Due to the large volume of attacks, the small payments add up substantially for attackers.

Blackmail scams are under-reported due to the intentionally embarrassing and sensitive nature of the threats. IT teams are often unaware of these attacks because employees don't report the emails, regardless of whether they pay the ransom.



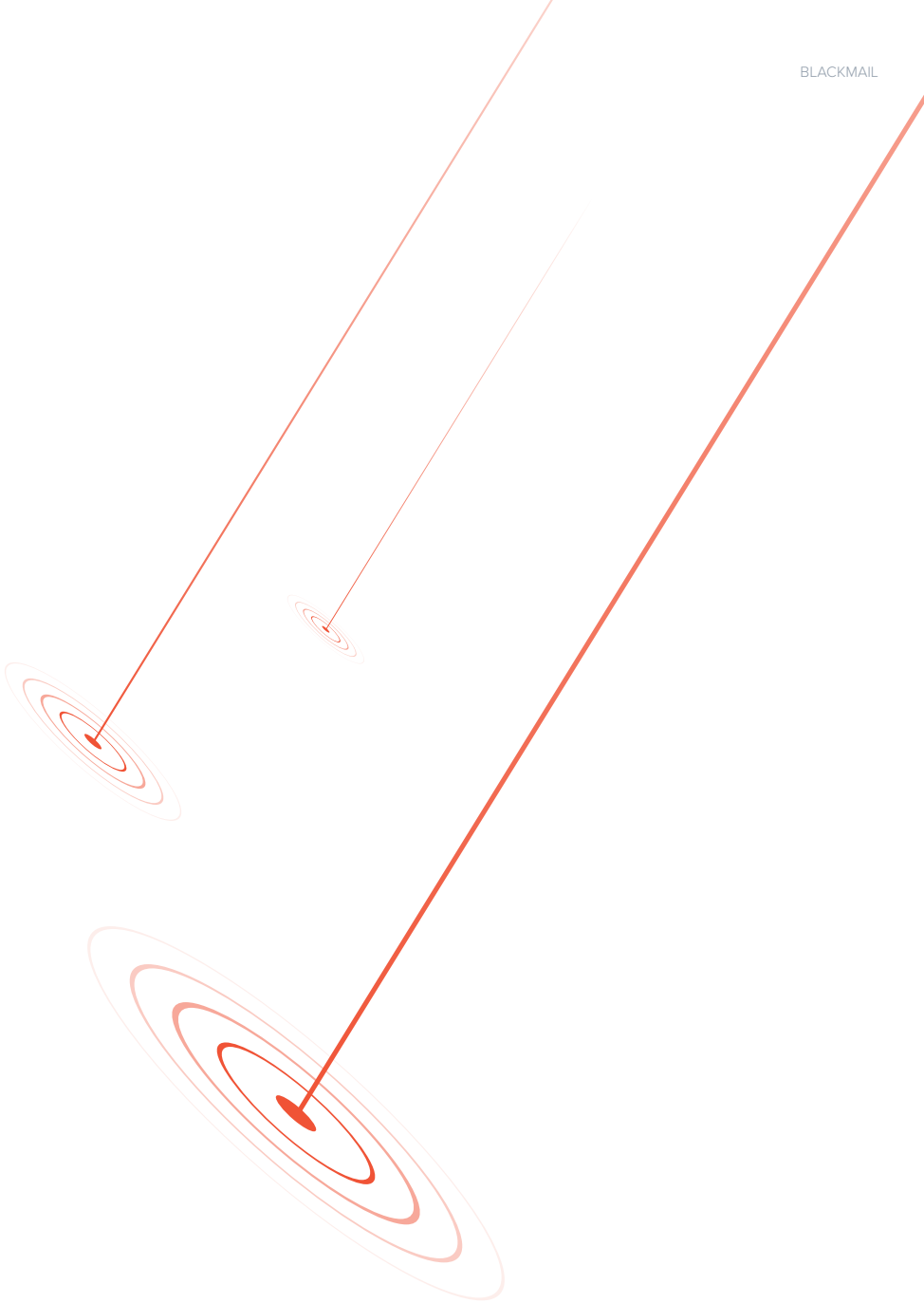
The cost of extortion and blackmail attacks continue to increase

Barracuda

Strengthening email defense against blackmail

Since inbox defense can access historical emails through APIs, it builds a statistical model of communication patterns, including the tone of voice used by individuals. This allows inbox defense to recognize the unusual and threatening tone of blackmail attacks, in combination with other signals, to flag it as malicious email.

While gateways can monitor for some signs of blackmail, such as the use of certain keywords, a lack of visibility into historical email data and the inability to recognize an abnormal tone of voice prevents them from protecting organizations from blackmail attacks.



Barracuda

Business Email Compromise

Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover

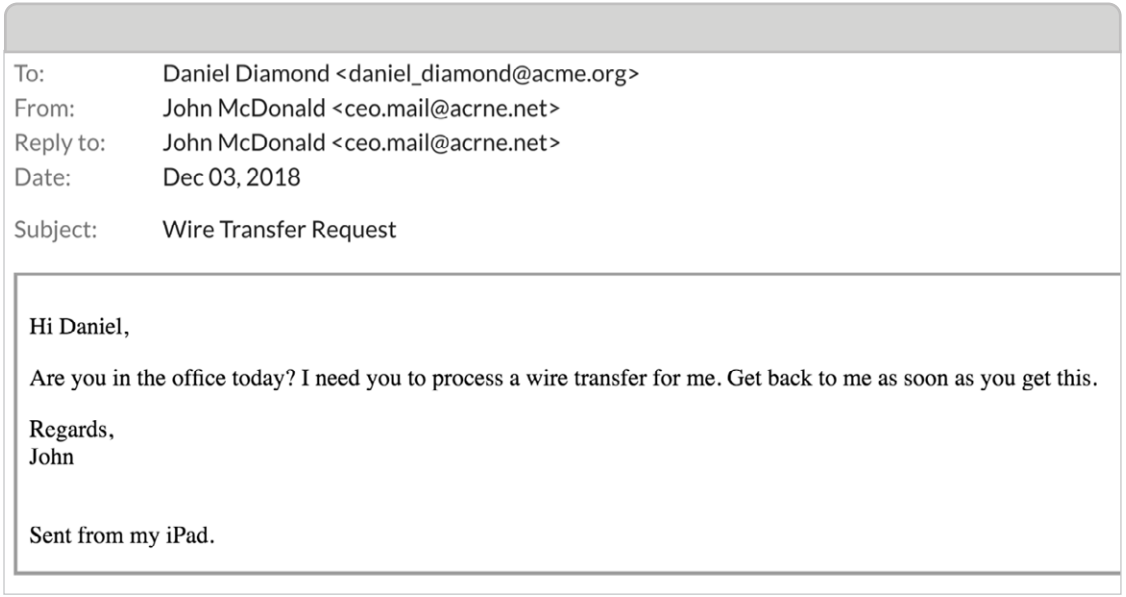
Less complex

More complex

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

Barracuda

In BEC attacks, also known as CEO fraud, whaling, and wire transfer fraud, scammers impersonate an employee in the organization in order to defraud the company, its employees, customers, or partners. In most cases, attackers focus their efforts on employees with access to the company's finances or personal information, tricking individuals into performing wire transfers or disclosing sensitive information. These attacks use social-engineering tactics and compromised accounts, and they often include no attachments or links.



To: Daniel Diamond <daniel_diamond@acme.org>
From: John McDonald <ceo.mail@acrne.net>
Reply to: John McDonald <ceo.mail@acrne.net>
Date: Dec 03, 2018

Subject: Wire Transfer Request

Hi Daniel,

Are you in the office today? I need you to process a wire transfer for me. Get back to me as soon as you get this.

Regards,
John

Sent from my iPad.

Example of an attack

Barracuda

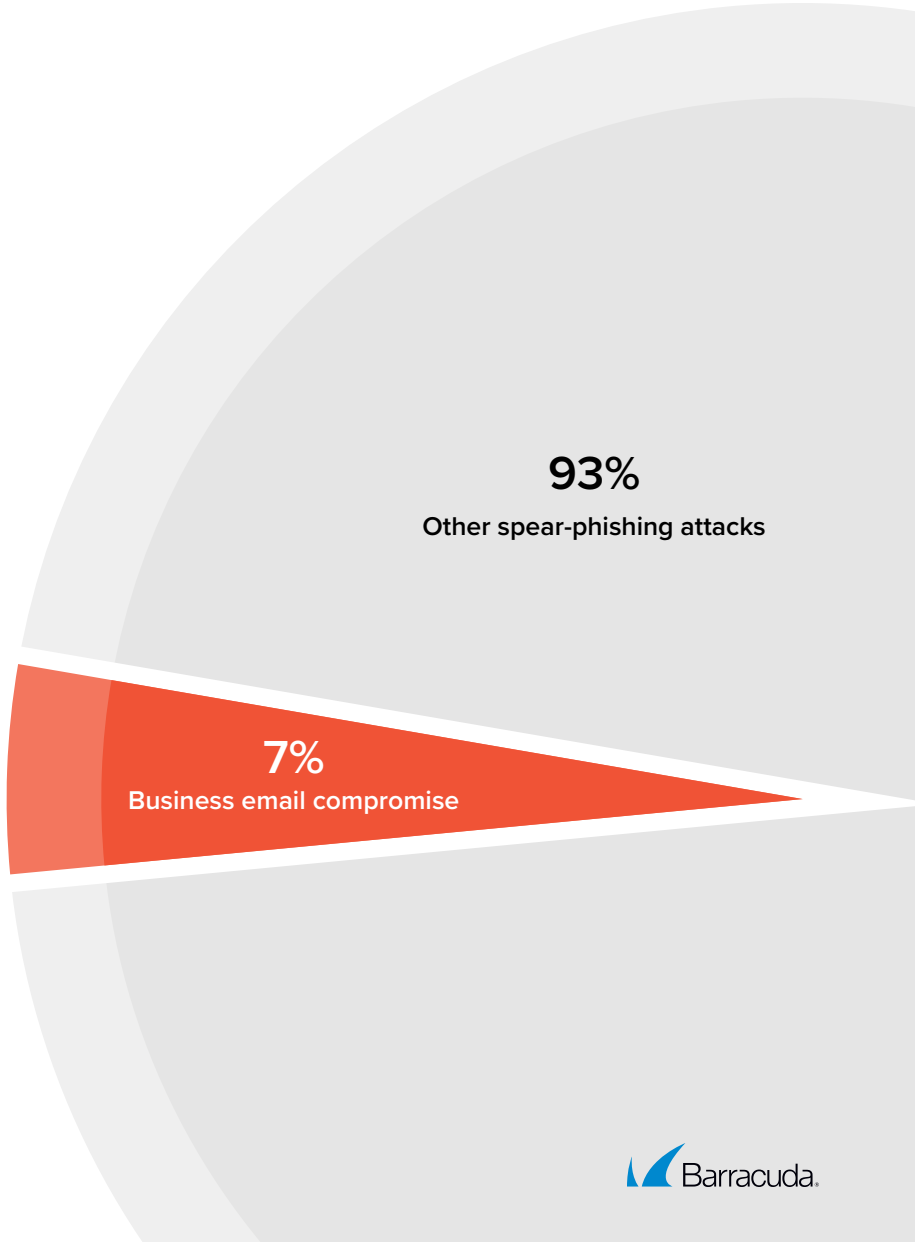
Impact of business email compromise

While business email compromise makes up only 7 percent of spear-phishing attacks, it caused more than $1.7 billion in losses in 2019 alone, according to the FBI. Gmail accounts are used to launch 47 percent of business email compromise attacks.

Payroll scams are a popular form of BEC attack. These scams target human resources and payroll departments with the goal of getting an employee's salary transferred to a different, fraudulent account. Hackers impersonate employees, providing new account details for the paycheck deposit. Payroll scams account for 8 percent of BEC attacks, but they are on the rise, growing more than 800 percent recently.

$1.7B

in losses in **2019**



Barracuda

Email defense against business email compromise

API-based inbox defense uses historical email data to build a statistical model or an identity graph to understand who is likely to communicate with each other and which names and identities they use. It also analyzes typical requests between employees within the organization using sentiment analysis. When an unusual request is made, API-based inbox defense identifies an impersonation attempt based on the history of communications, rather than the rules and policies relied on by traditional email gateways.

Email gateways have no visibility into relationships and communication patterns between individuals based on historical data. Gateways rely on customized granular policies and DMARC for spoofing and impersonation protection. These techniques are not enough to protect against BEC, and their overreliance on predetermined policies leads to large numbers of false positives or negatives. API-based inbox defense is a more effective protection against BEC attacks.

"The most advanced solutions analyze historical communication patterns and detect potential impersonations based on these."

Source: Gartner, March 2020

Barracuda

Conversation Hijacking

Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover

Less complex

More complex

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

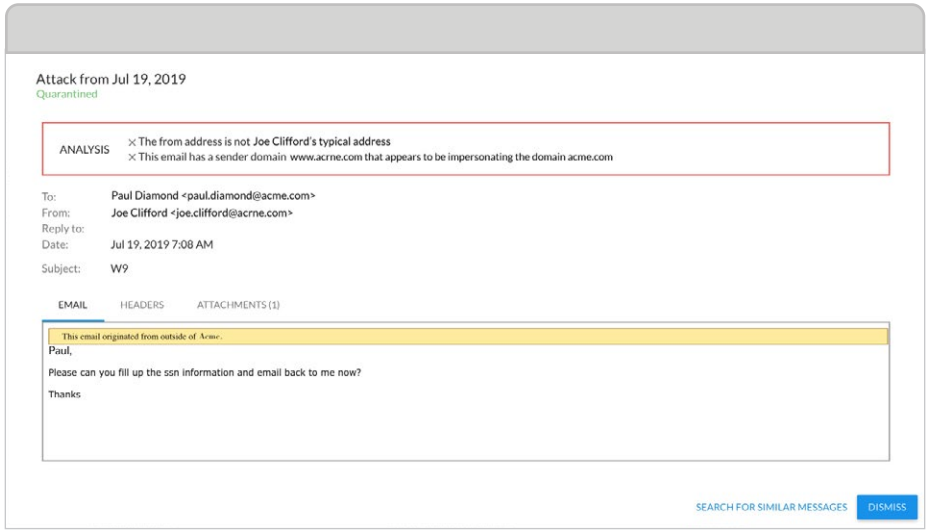
Barracuda

With conversation hijacking, cybercriminals insert themselves into existing business conversations or initiate new conversations based on information they've gathered from compromised email accounts to steal money or personal information.

Conversation hijacking can be part of an account-takeover attack. Attackers spend time reading through emails and monitoring the compromised account to understand business operations and learn about deals in progress, payment procedures, and other details.

Cybercriminals rarely use the compromised accounts to send a conversation hijacking attack, though. Instead, attackers use email-domain impersonation.

Here's an email showing how cybercriminals try to impersonate an internal email domain during an attempted conversation-hijacking attack.



Example of an attack

Barracuda

Impact of conversation hijacking

In recent months, there's been a sharp rise of more than 400 percent in domain-impersonation attacks used to facilitate conversation hijacking. While the volume of conversation hijacking in domain-impersonation attacks is extremely low compared to other types of phishing attacks, these sophisticated attacks are very personalized, making them effective, hard to detect, and costly.

In one well-publicized case, the Shark Tank's Barbara Corcoran lost nearly $400,000 due to a phishing scam. Scammers tricked her bookkeeper using email-domain impersonation, sending a bill that appeared to come from her assistant. But Corcoran's assistant never sent the invoice; the fake bill came from an email that closely resembled her address. By the time Corcoran's team realized something was wrong, the money had already been transferred to the scammers.

$400K

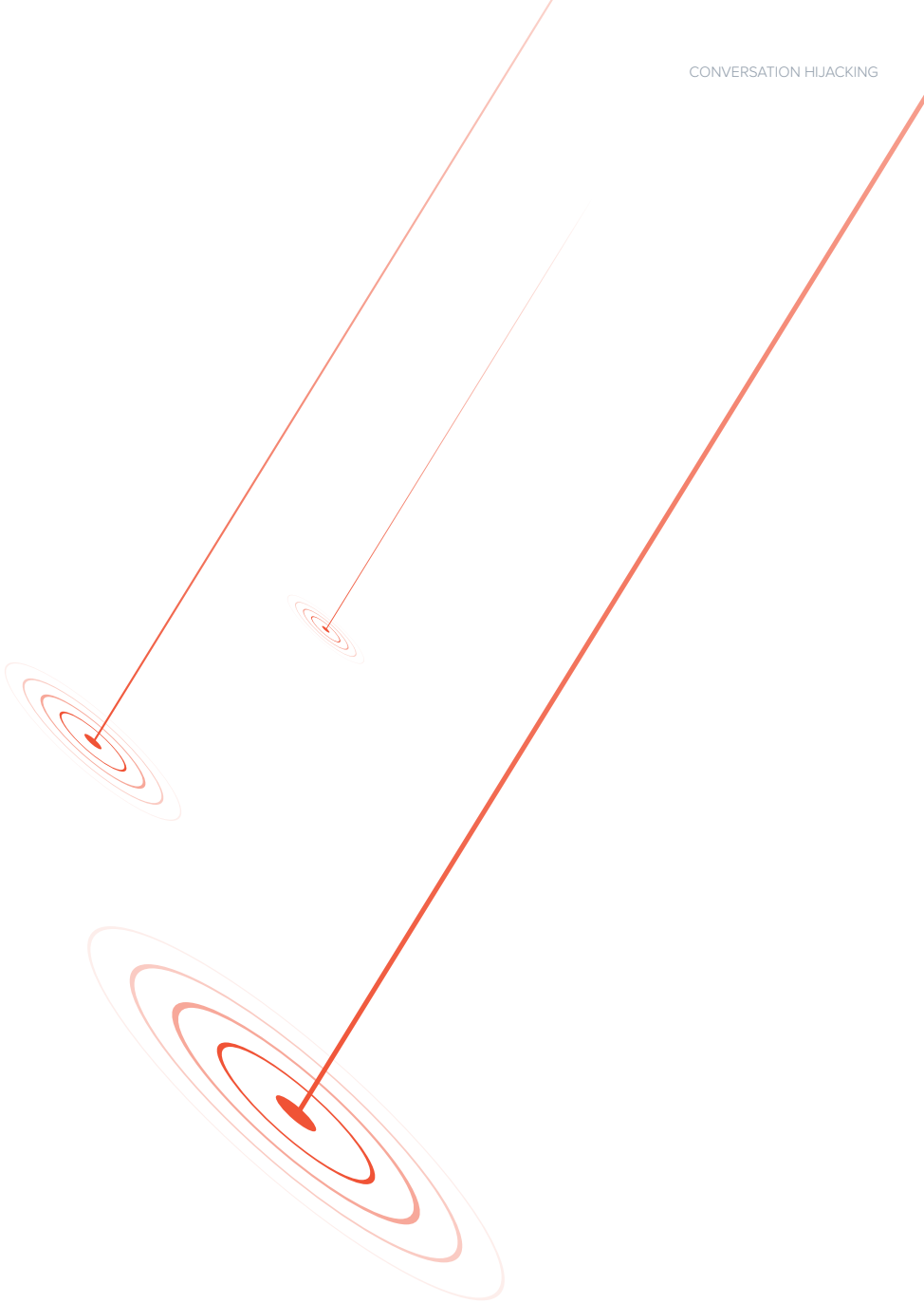
Lost by Shark Tank's Barbara Corcoran in a conversation-hijacking attack

Barracuda

Strengthening email defense against conversation hijacking

Inbox defense gains access to historical email communications through API integration, using that data in machine learning to understand who is likely to communicate with who, including usual external contacts and interactions with them. When an email conversation is hijacked and a trusted partner is impersonated by cybercriminals, inbox defense blocks the attack.

Gateways have none of that visibility. While policies and white lists can be created, this approach is difficult to scale and can lead to false positives. When a conversation is hijacked, the gateway delivers the email. Therefore, the gateway is unable to protect against this type of attack.



Barracuda

Lateral Phishing

Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover

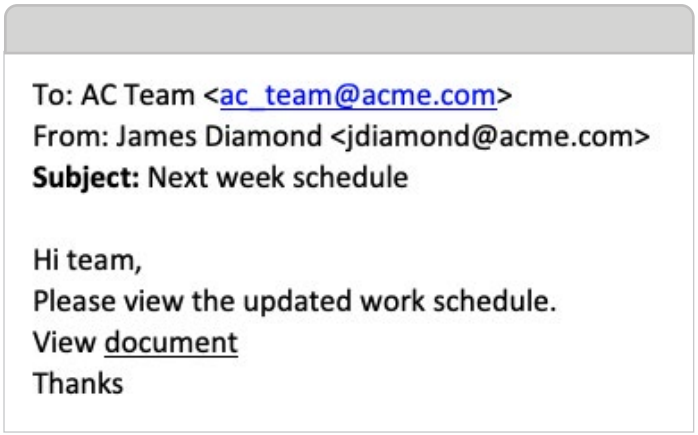
Less complex

More complex

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing

Barracuda

With lateral phishing, attackers use recently hijacked accounts to send phishing emails to unsuspecting recipients, such as close contacts in the company and partners at external organizations, to spread the attack more broadly. Because these attacks come from a legitimate email account and appear to be from a trusted colleague or partner, they tend to have a high success rate.


To: AC Team <ac_team@acme.com>
From: James Diamond <jdiamond@acme.com>
Subject: Next week schedule

Hi team,
Please view the updated work schedule.
View document
Thanks

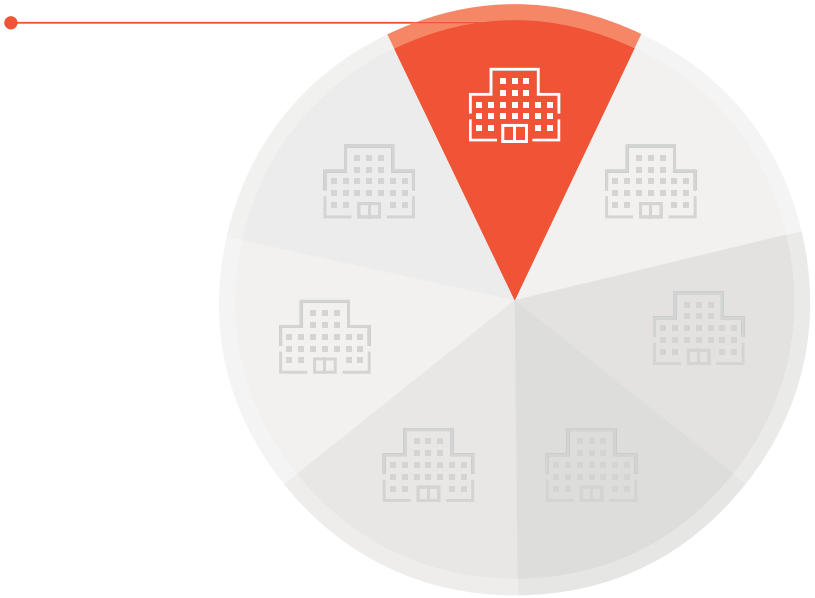

Dear user,
We noticed an error on your account, kindly rectify click here. Sorry for the inconvenience.

Examples of an attack

Impact of lateral phishing

In a recent study, researchers found that 1 in 7 organizations has experienced a lateral phishing attack. These attacks, targeting a wide range of victims and organizations, can be extremely damaging to a business's brand reputation, especially if they lead to additional widespread attacks in other organizations.

More than 55 percent of these attacks target recipients with some work or personal connection to the hijacked account. Not surprisingly, about 11 percent of these attacks successfully manage to compromise additional accounts, leading to even more lateral phishing attacks.



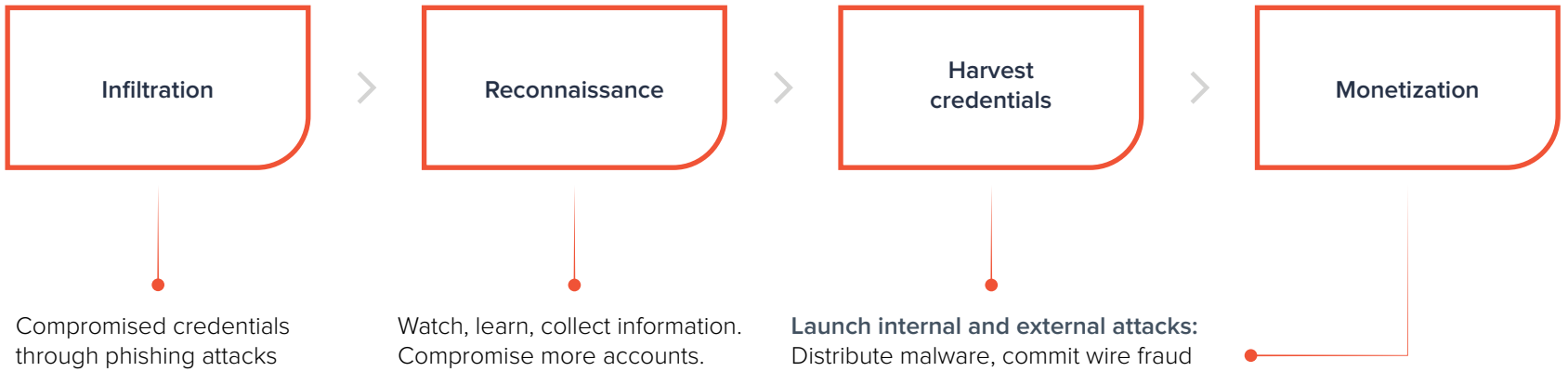
1 in 7 organizations has experienced a lateral phishing attack.

Strengthening email defense against lateral phishing

In most cases, lateral phishing is an internal attack. Email gateways have no visibility into these communications and can't stop internal attacks because they never pass through it. Gateways can't remediate attacks post-delivery, either. Once email is delivered to the inbox, it stays there. APIs for inbox defense provide visibility into internal communications. They can detect internal threats, such as lateral phishing, and remediate them post-delivery.


Account
Takeover
admin
Spam
Data Exfiltration
Scamming
Domain Impersonation
Blackmail
Conversation Hijacking
Account Takeover
Less complex
More complex
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing
Barracuda

Account takeover is a form of identity theft and fraud, where a malicious third party successfully gains access to a user's account credentials. Cybercriminals use brand impersonation, social engineering, and phishing to steal login credentials and access email accounts. Once the account is compromised, hackers monitor and track activity to learn how the company does business, the email signatures they use, and the way financial transactions are handled. This helps them launch successful attacks, including harvesting additional login credentials for other accounts.

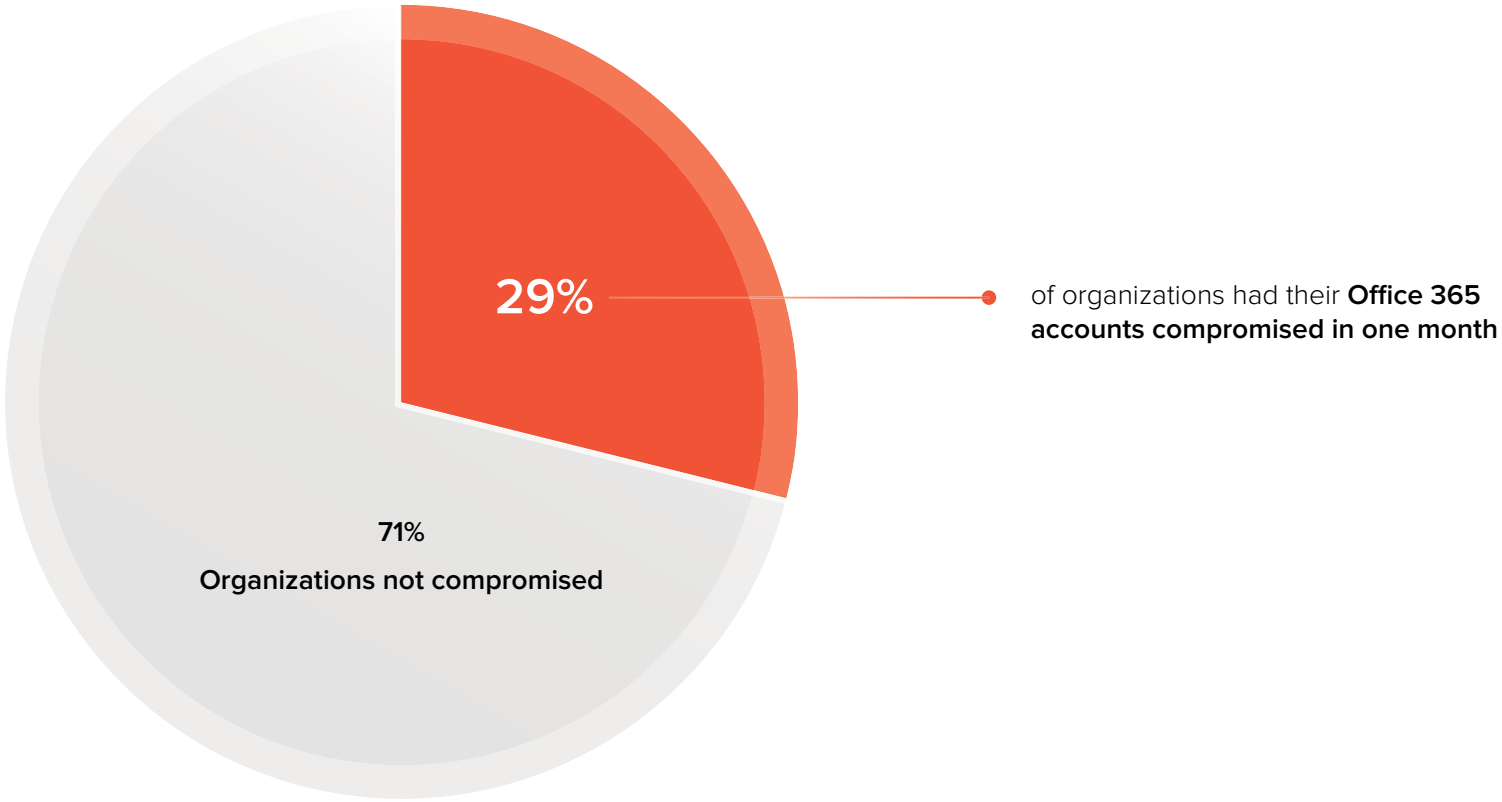


How an account takeover attack happens

Barracuda

Impact of account takeover

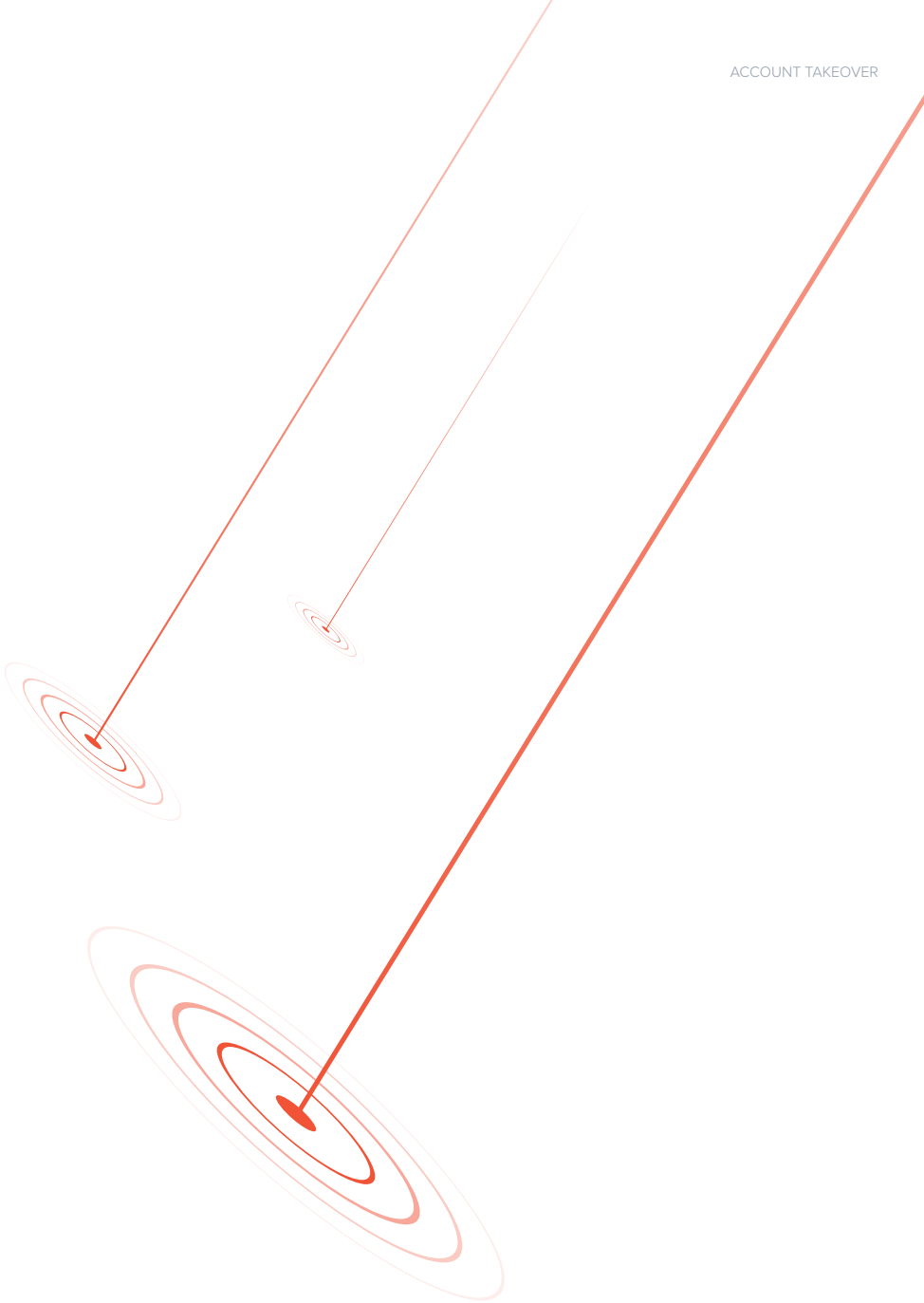
A recent analysis of account-takeover attacks found that 29 percent of organizations had their Office 365 accounts compromised by hackers in one month. More than 1.5 million malicious and spam emails were sent from the hacked Office 365 accounts in that 30-day period.



Barracuda

Email defense against account takeover

Gateways are positioned on the perimeter, outside of an organization, so they are disconnected from email inboxes and users. They lack the ability to monitor for suspicious behavior, such as logins from unusual locations or messages forwarded internally. An API-based inbox defense connects directly with users' inboxes, monitoring for suspicious changes to inbox rules, unusual login activity, and malicious messages sent from already-compromised accounts. Inbox defense detects account takeover before it's used to conduct fraud and remediates an attack by locking malicious users out of the compromised account.



Barracuda

Strengthening your email security posture with API-based inbox defense

Traditional email gateway security

The email gateway is a security perimeter that sits in front of your mail server and is designed to filter inbound and outbound email messages for malicious content. Email gateways use technologies like reputation filters to look for low-reputation IPs. They evaluate email content for signs of malicious intent, scan for viruses and malware, authenticate the sender, and analyze URLs, blocking any that will lead to phishing sites or sites designed to distribute malware. Email gateways are very effective at detecting and blocking zero-day attacks and ransomware. This layer of protection includes advanced threat protection technologies, such as sandboxing, which evaluates new, never-before-seen variants of malware in a controlled environment.

Gateways are the necessary foundation of email security. They block most malicious messages, including spam, large-scale phishing attacks, malware, viruses, and zero-day attacks.

However, because of their overreliance on filters, rules, and policies, gateways fall short of protecting your organization from highly targeted email attacks that use social-engineering tactics, including spear phishing and business email compromise. Gateways look for signs of malicious content or senders, but they let through attacks that don't trigger any of their predetermined policies, filters, or authentication rules.

API-based inbox defense

While email gateways are still necessary, they are no longer enough to protect against evolving cybersecurity threats. To protect your organization from socially engineered attacks, you need an additional layer of defense—beyond the gateway and at the inbox level.

Inbox defense relies on APIs to integrate directly with your email environment, including individual inboxes. Using API integration provides visibility into both historical and internal

"Upgrade secure email gateway solutions to include advanced phishing protection, imposter detection and internal email protection."

Source: How to build an effective email security architecture, Gartner, March 2020

Barracuda

email communication for every individual in the organization. It then uses this communication data and artificial intelligence (AI) to create an identity graph for each user that reflects their communication patterns.

The identity graph is built using multiple classifiers that determine what normal email communications look like for each employee. For example, it understands (based on historical data) which locations each employee is likely to log in from, their regular email addresses, individuals they communicate with, the type of requests they make, and hundreds of other signals. When something abnormal happens that is outside of an individual's identity graph, AI within your inbox defense flags it as potentially malicious and removes it from the user's inbox before they can interact with the message.

While you can get email gateways to behave in a similar way, that solution doesn't scale. Many of today's email gateways allow for granular customization and policy settings to block targeted attacks. Each classifier can potentially be turned into a rule or policy for the gateway, but with hundreds of policies that need to be set up for thousands of employees, the solution doesn't scale. It's not adaptable to change, and it's prone to a large number of false positives and negatives. Organizations relying on customized gateways to protect their users from spear-phishing attacks are only able to protect a select number of employees who have been identified as high risk. Inevitably, spear-phishing attacks will bypass their gateways and make it into users' inboxes.

Email Threat Taxonomy - 13 Threat Types

THREAT TYPES	EMAIL GATEWAY	API-BASED INBOX DEFENSE
Spam	●	○
Malware	●	○
Data Exfiltration	●	○
URL Phishing	◑	●
Scamming	◑	●
Spear Phishing	○	●
Domain Impersonation	○	●
Service Impersonation	○	●
Blackmail	◑	◑
Business Email Compromise	○	●
Conversation Hijacking	○	●
Lateral Phishing	○	●
Account Takeover	○	●

○ Does not provide sufficient protection ◑ Provides some protection ● Provides best protection

Barracuda

Conclusion: Effectively protecting against evolving email threats

Email attacks have evolved to bypass traditional defenses and require organizations to set up protection, not only at the gateway, but also beyond it. Every business needs to deploy the right combination of technology and people to have effective email protection.

Block high-volume attacks at the gateway

Gateways are the necessary foundation of email security. They block most malicious messages, including spam, large-scale phishing attacks, malware, viruses, and zero-day attacks. If these attacks go unchecked, they wreak havoc inside your organization, impacting productivity and infecting machines.

Protect your users at the inbox level

Although gateways are important, they are no longer sufficient on their own. Deploying API-based inbox defense unlocks access to historical and internal email communication, which is necessary to protect your users against the highly targeted attacks that slip past gateways.

Educate users on the latest threats

Some evolving and sophisticated phishing attacks, including those that use social-engineering tactics, can slip through the secure email gateway. Guard against these types of threats with security awareness training for employees. With continuous simulation and training, employees are able to recognize and report malicious content, transforming them into a layer of defense.

Barracuda
Your journey, secured.